CONFERENCE ON PRIVACY:

INITIATIVES FOR 1984

TORONTO, ONTARIO, CANADA
MAY 22 - 25, 1984

Provincial Secretariat For Resources
Development, Ontario
1984

Available Through The
Ontario Government Bookstore
880 Bay Street
Toronto, Ontario
M7A 1N8

Copies de documents
Son disponsibles en francais
appelez Rudy Wall,
Secretariat de la province
au Developpement des Ressources
(416) 965-1902

Edited by: Rudy Wall
Policy Advisor
Provincial Secretariat for
Resources Development.

Canadian Cataloguing in Publication Data

Conference on Privacy, Initiatives for 1984 (1984 : Toronto, Ont.)
Conference on Privacy, Initiatives for 1984, Toronto, Ontario, Canada, May 22-25, 1984. --

ISBN 0-7743-9566-4

1. Privacy, Right of--Congresses. I. Ontario. Provincial Secretariat for Resources Development. II. Title.

JC596.C6 1984 323.44'8 84-093031-3

TABLE OF CONTENTS

	PAGE
MESSAGE FROM THE MINISTER: The Honourable Norman W. Sterling, Q.C. Provincial Secretary for Resources Development	v
EDITOR'S NOTE	vi
PART A: ONTARIO GREEN PAPER	
DISCUSSION PAPER ON PRIVACY: INITIATIVES FOR 1984 Rudy Wall, Policy Adviser Secretariat for Resources Development, Ontario Martha Fletcher, Policy Advisor Ministry of Transportation and Communications, Ontario	2
PART B: MAJOR CONFERENCE ADDRESSES	
KEYNOTE SPEECH ON PRIVACY: INITIATIVES FOR 1984 The Honourable Norman W. Sterling, Q.C. Provincial Secretary for Resources Development, Ontario	20
PROTECTION OF PERSONAL INFORMATION IN THE U.K.: THE DATA PROTECTION BILL The Honourable David Waddington, Q.C. Minister of State for the Home Office, United Kingdom	24
THE PRIVACY ACT: HOW IS IT WORKING TO DATE? Dr. John W. Grace, Privacy Commissioner of Canada	30

PAGE

PART C: CONFERENCE PANELS

PANEL 1: PRIVATE SECTOR PANEL: "PRIVACY: THE PROBLEMS DEFINED" 36

PANELISTS: James L. Kirschbaum, Chairman and C.E.O., Fireman's Fund Insurance Company of Canada Ltd., Toronto (representing the Insurance Bureau of Canada) 37

Dr. William R. Ghent, Chairman, Council on Health Care The Canadian Medical Association Ottawa 41

Ross McFarlane, Q.C., General Counsel, General Motors of Canada, Toronto (representing the Canadian Manufacturer's Association) 44

PANEL 2: PUBLIC SECTOR PANEL: "ACCESS TO INFORMATION: HOW DOES THIS RELATE TO PRIVACY?" 50

PANELISTS: John D. McCamus, Dean, Osgoode Hall Law School, York University, Toronto 51

Professor T. Murray Rankin, Faculty of Law, University of Victoria, Victoria 62

Professor David Flaherty, Privacy Project, University of Western Ontario, London, Ontario 67

PANEL 3: PRIVATE SECTOR PANEL: "PRIVACY: WHAT THE PRIVATE SECTOR HAS DONE" 73

PANELISTS: Ralph Hancox, President Readers Digest Association of Canada, Montreal 74

Robert G. Logan, Director External Programs, IBM Canada Limited, Toronto 80

Eric Wimberley, Canadian Cable TV Association, Ottawa 84

		PAGE
PANEL 4:	PUBLIC SECTOR PANEL: "PRIVACY: SOME PRACTICAL SOLUTIONS"	87
PANELISTS:	Hugh V. O'Neill, President, American Society of Access Professionals, Washington, D.C.	88
	Caroline Pesticau, Commission d'access a l'information du Quebec, Montreal	91
	Douglas D. Smith, Assistant Deputy Minister Communications Policy Branch, Department of Justice, Saskatchewan	96
PANEL 5:	"PRIVACY: INITIATIVES FOR THE PRIVATE SECTOR"	100
PANELISTS:	W.H. Loewen, President, Canadian Independent Computer Services Association, Winnipeg	101
	Boris Mather, Canadian Federation of Communications Workers, Ottawa	104
	Maryon Brechin, Consumers' Association of Canada, Ottawa	105
PANEL 6:	"TRANSBORDER DATA FLOW: TOWARD A RESOLUTION FOR THE FUTURE: THE TRENDS, THE ISSUE"	109
PANELISTS:	Professor Thomas L. McPhail, Ph.D. Director and Professor, Graduate Program in Communications Studies, The University of Calgary	110
	Jan K. Fedorowicz, Canadian Representative, International Chamber of Commerce, Ottawa	124
	James C. Grant, Vice-President, Strategic Planning, Retail Banking, The Royal Bank of Canada, Ottawa	130

PAGE

SUMMATION BY CONFERENCE RAPPORTEUR 135

Carl F. Dombek
Director, Legal Services
Ontario Ministry of Labour

MESSAGE FROM THE MINISTER

I am happy to introduce to you the Proceedings from the "Conference on Privacy: Initiatives for 1984", which was held in Toronto during May of 1984.

I would like to express my thanks to all the Conference Speakers and Panelists for their contributions at this Conference. I would also like to thank all those who assisted in the organizational tasks and who helped make the event a success.

In reading the papers presented in this volume, one is impressed by the complexity of the Privacy issue. It is apparent that one set of rules developed for one industry or company to protect personal information files may not be appropriate for another.

I was encouraged to hear from many private sector delegates at the conference that they favour a self-regulatory solution to privacy concerns. It is apparent that companies and industry associations want the opportunity of developing voluntary privacy codes and fair information practices.

I hope that this Conference Proceedings book will give some "food for thought " for this task and am convinced that the development of voluntary codes would greatly increase public confidence in information handling practices.

Yours sincerely,

Norman W. Sterling, Q.C.
Provincial Secretary
for Resources Development

EDITOR'S NOTE

The organization of this document reflects the desire to reproduce the proceedings of the Conference in as direct and true a form as possible.

The document begins with Ontario's Green Paper on the subject of informational privacy in the computer age. This is followed by a section containing the three major speeches, which set the tone for each part of the Conference.

The six panels are then presented in chronological order. The panels consisted of introductory remarks by the Chairman, presentations from three panelists and a wrap-up by a panel commentator. You will note that panels were also divided into two major streams: those dealing with public sector legislation and those dealing with the issue of personal data protection in the private sector.

The summary section contains the remarks of the Conference Rapporteur at the close of the Conference. This chapter can serve as a useful synopsis for the reader who does not have time to go through the entire document.

I would like to thank the conference speakers and Panelists for submitting their presentations in written form, making possible the publication of this book. I hope it will be of assistance in bringing together the many diverse views on this important subject.

Rudy Wall
Policy Advisor
Provincial Secretariat
for Resource Development

PART A

ONTARIO GREEN PAPER

DISCUSSION PAPER ON PRIVACY: INITIATIVES FOR 1984

RUDY WALL *
Policy Advisor
Secretariat for Resources
Development, Ontario

MARTHA FLETCHER **
Policy Advisor
Ministry of Transportation
and Communication, Ontario

SYNOPSIS

Developments in computer and telecommunications technology have raised new questions about informational privacy - the capacity for individuals to determine what information is collected about them and the manner in which it is made available to others. This Discussion Paper introduces the reader to some of the major issues raised by the potential impact of technological developments on privacy and discusses some alternative approaches to their resolution.

These issues centre on data collection, data quality, disclosure limitations, security safeguards, costs and individual access to personal records in computerized data banks. Recent surveys of public attitudes suggest that individuals are very concerned about computers affecting personal privacy and about institutions collecting too much personal information.

The public sector has begun to address these problems with various statutes which establish and enforce fair information practices for data banks held by government departments and agencies. Examples include Canada's Federal Privacy Act and Quebec's Bill 65, both of which also establish offices to ensure compliance with privacy standards and consider individual complaints regarding information practices.

Ontario has introduced for First Reading Bill 80, the Privacy and Access to Information Act, that would seek to establish fair information practices for provincial government data banks. It would set up a compliance office as well as an office to receive citizen's complaints regarding information practices.

---

* Mr. Wall has served in various policy positions in the Ontario Government, including the position of Chief Economist at the Ministry of Consumer and Commercial Relations. Prior to entering the Ontario Public Service, Mr. Wall was an Instructor at Ryerson Polytechnical Institute, Toronto, in the Department of Business and Technical Communication.

** Ms. Fletcher is in the Communication Division, Ontario Ministry of Transportation and Communications. Formerly in the Political Science Department, York University, she has written extensively on public law and public policy issues in the Canadian context, with emphasis on constitutional law, federalism and telecommunications policy.

Data protection has received much attention in Europe, where countries like the United Kingdom, West Germany and Sweden have legislative programs which register data banks and regulate information practices in both the public and private sectors.

The private sector has shown sensitivity to privacy concerns by developing internal practices and, in some cases, voluntary privacy codes which embrace some of the principles commonly found in data protection laws. In the United States, Warner-Amex Cable Communications Inc. has developed a code to protect the privacy of the personal information it gathers on its customers. The Canadian Cable Television Association is in the process of developing a privacy code with similar self-regulation objectives.

Traditionally, credit bureaus, which are regulated in most provinces by credit reporting Acts, have been the main handlers of personal information in the private sector. However, the growth of computerized personal information banks can be seen in a wide range of industries including financial institutions, cable TV services as well as a host of other business and non-business sectors. The individual has no concrete guarantees against infringements of informational privacy in these data banks.

In order to develop a uniform approach to the privacy problem, Canadian jurisdictions will have to grapple with a number of legal issues. These include questions such as: Who owns the information in personal data banks? How should that information be legally protected? Do existing privacy laws need to be amended in light of the expanding technology? Does liability ensue from an improper or unauthorized release of personal information?
Then, of course, there is the everlasting problem of jurisdiction between the federal, provincial and territorial governments to harmonize rules as they are developed and to avoid any conflicts in the laws.

It is a generally held view that individual rights, including privacy rights, are not within the exclusive legislative competence of either the Federal or Provincial levels of government but rather are determined by the Canadian Constitution and more particularly S.91 and S.92 of the B.N.A. Act. Although a number of governments already have Privacy Statutes, it is important that these initiatives continue and perhaps expand.

This paper analyzes four approaches to resolving privacy concerns brought about by the growth in computerized handling of personal information in the private sector. Instead of reviewing the whole spectrum of possible approaches, it focuses on four that are thought to be suitable for the Canadian situation.

The Government has developed a strong role in promoting and adopting microelectronic and communications technology. It therefore has a complementary responsibility to ensure that privacy standards are upheld as the technology is adopted in all sectors of the economy.

The first possible approach would be for government to encourage self-regulation in industries which are important data users. This could take the form of voluntary privacy codes modelled after those used by companies discussed later in this report. The most noteworthy attempts at self-regulation also include provisions regarding fair information practices in their customer agreements Government could work with a representative association in each industry sector in developing a privacy code for that sector. This would produce a series of voluntary privacy codes tailored to fit the requirements of each sector.

A second possibility would be for government to develop legislation which sets out fair information practices and includes a penalty provision for the offense of violating these practices. This could be voluntary in form, covering only those firms which wish to comply, or it could be compulsory, including all important data users in the private sector.

A third possible alternative is to set up a registration and regulation system governing data users. Such a system could set out major principles regarding information handling; set up a Registrar or Commissioner's Office to administer the registration system and ensure compliance with principles; and establish individual rights to access, correction and non-disclosure of personal information. Models of registration systems include the United Kingdom Data Protection Bill as well as systems set up by Canadian provinces to regulate personal credit information.

Combinations of these three approaches would yield other possibilities. One such possibility which is worthy of analysis is a combination of the Self-regulation and Registration approaches described above. For the purposes of this paper, this has been called the "Voluntary Registration" approach. Industry associations could develop privacy codes tailored to their industry, monitor compliance among their members, and mediate complaints from individual citizens. This could be done in consultation with a public Privacy Office which could also keep a registry of all participating associations and companies.

PART I: UNDERSTANDING THE ISSUES

Introduction

The need for informational privacy - the capacity for individuals to determine, in significant measure, what information is collected about them and the manner in which it is made available to others - has long been recognized as a legitimate aspect of a free society. Yet, though the importance of privacy as a value has been widely accepted, its existence has depended in large part on the technological impossibility of detailed surveillance and record-keeping about large numbers of individuals. That technological barrier no longer exists. Therefore, standards will now have to be considered if informational privacy is to be maintained in the face of technological advance.

Key to the creation of such safeguards is the development of a consensus regarding fair information practices. These practices would generally define limits on the way personal information is collected, stored and used. They would also attempt to balance the individual's privacy with competing social values of openness and economic values of efficiency. For the purposes of this paper, personal information may be defined as information in a record about an individual person where that person is identified by name or is readily identifiable by other means.

The purpose of this Discussion Paper is to introduce the reader to the major issues raised by the potential impact of technological developments on individual privacy and to discuss some of the alternative approaches to their resolution.

Recent developments in computer and telecommunications technology have made it possible to process and link information held in a variety of data banks with ease, low cost and speed. In the past quarter century record-keeping by both government and private entities has moved from the slow, clumsy era of paper files, where information is entered manually, to high speed, efficient, machine-readable files. This development has had a number of significant implications for privacy.

First, machine-readable files are more quickly retrieved and more readily and anonymously updated. What was once a collection of pieces of paper, with the age of each readily apparent, is now a computer readout. Moreover, computer files are easily accessible from many distant points in the organization. More important, however, is the fact that computerized files are readily merged, allowing a number of files dealing with the same subject or individual to be compiled into a single dossier. This can be done within the organization which collected the data. However, data can also be easily transferred to another information user and combined with other files from other sources for uses

not envisioned by any of those persons associated with the initial information -gathering process. This is made easier by the use of a single identifying number, but the absence of such a number is not a significant bar to such compilations. In addition, telecommunication links between the holders of files make it possible for the files collected by one institution for one purpose to be shared with other information users for quite different purposes. This process is called data linkage.

The potential impact of efficient retrieval, sharing and merging of files on informational privacy is magnified by the sheer number and variety of sources of computerized information about individuals. The physical size of computers has dropped in twenty years from room-sized machines to ones which fit easily on a desk top. Costs of machinery and processing have dropped at a comparable rate. The older generation of machinery required extensive training to use; present equipment, dubbed "user friendly", can be operated with little specialized training or knowledge.

Where once only the largest institutions, including government, had the resources to effectively use the computer, computerized record keeping is now the norm in virtually every area of human activity. Once the national census was the sole compilation of varied facts about individuals. Now it is possible to compile even more varied information about individuals by the sharing of information among file holders. In government, files held on individuals include information on vital statistics, tax, criminal and court proceedings, health, driving, military and school records, among others.

In the private sector, information held on individuals in computerized files is even more varied. Among the best-known is the credit-rating file. However, the public is becoming aware of other computerized files including those in the insurance, banking and telecommunication industries. In addition, there are many data users of which the public is unaware: retail sellers who have credit card systems or teleshopping services; magazines which keep subscription lists; charitable, business, professional or community organizations; and many other service providers. As cable television companies enter into two-way operations which make it possible for the consumer to undertake telebanking, teleshopping, and instant polling, and order television programs on a "pay per view" basis, greater amounts of personal data will be stored by the private sector.

This all pervasive collection of personal information is a virtually unavoidable feature of life in the last quarter of the twentieth century. As the U.S. Privacy Protection Study Commission concluded in 1977:

> It is now commonplace for an individual to be asked to divulge information about himself for use by unseen strangers who make decisions about him that directly affect his everyday life. Furthermore, because so many of the services offered by organizations are, or have come to be considered, necessities, an individual has little choice but to submit to whatever demands for information about him an organization may make.

Fair Information Practices

This threat to privacy has resulted in a number of attempts to define appropriate limits and to protect the privacy of personal information stored in computer systems. The general principles enunciated in the Council of Europe's "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" are typical of efforts in a number of jurisdictions to establish guidelines which recognize the benefits of computerized record keeping and the value which individuals place on personal privacy. These guidelines include the following concepts:

i) Personal information should be obtained and processed fairly and lawfully;
ii) Personal information should be held for a specified and legitimate purpose or purposes;

iii) Personal information should not be used or disclosed in a way incompatible with those purposes;

iv) Personal information should be adequate, relevant, and not excessive in relation to the specified purposes;

v) Personal information should be accurate and, where necessary, kept up to date;

vi) Personal information should be kept in name linked form for no longer than is necessary for the specified purposes;

vii) The data subject should have access to information held about him or her and be entitled to its correction or erasure where the legal provisions safe-guarding personal data have not been complied with;

viii) Appropriate security measures must be taken against unauthorized access, alteration or dissemination, accidental loss and accidental or unauthorized destruction of data.

These guidelines recognize the individual's need to ensure that information which is gathered about him is done so with his consent; that this consent is given with a full and accurate understanding of the purpose for which the information is gathered; that other uses will not be undertaken without prior consent; that the file will be made available so that the individual can ensure the information is correct; that, in the event there is disagreement about the accuracy of the information, the data subject's version will be noted; and that third parties will not be given access without the individual's knowledge or permission except where required by law.

Even where there is general agreement with these principles in both the public and private sectors, however, there are a number of impediments to their fulfillment. One of these is the companion principle of freedom of information. If an individual has full control over all his personal information, this right can present a major barrier to the rights of others to obtain information on government activities. Clearly a balance must be struck.

Another impediment is the problem of computer crime, where data is taken or released without the permission of the data bank owner. It has been suggested that criminal code amendments which would establish specific offences relating to computer crime would go part way to solving this problem. However, owners of data banks would still have to take reasonable precautions inside their organizations to ensure that personal information is kept confidential and that employees handling this information follow necessary safeguards.

A third potential impediment is the problem of transborder data flow, when information relating to individuals is removed to and processed in another jurisdiction where privacy is not adequately protected by business practices or by law. Here again efficiency and the value of the free flow of information may come into conflict with privacy norms. Certain of these issues are beyond the scope of this discussion since they fall within the realm of the Federal Government.

Public Perceptions

Recent surveys indicate that concerns about privacy brought on by growing computer use are not the sole preserve of academics, futurists, and policy makers. Surveys conducted for the Ontario Government in 1980 and 1983[1] show that a considerable majority of Ontario citizens are concerned about computers affecting personal privacy. In addition, in 1983, about half the population felt that government has the major responsibility for ensuring confidentiality of personal and financial information in our society. An additional 38 percent saw the private sector as having major responsibilities for privacy protection. The earlier 1980 survey further revealed that a sizeable minority believe that institutions such as government, credit-grantors, employers and insurance companies ask individuals for too much personal and financial information.

As well, a 1981 Gallup[2] survey on attitudes toward microelectronic technology

asked respondents to indicate the importance of thirteen issues associated with computers and information technology. Privacy and confidentiality of personal information was by far the most important of the issues and was mentioned by 63 percent of the respondents. The number of people controlling information, a closely related issue, was third in importance, mentioned by 45 percent of respondents. Concern for privacy was highest among those who reported that they had knowledge of microelectronics and among respondents who held executive, sales and clerical jobs. Individuals were also asked to look ahead for the next five years and predict whether or not their privacy would be "invaded or seriously disturbed" by any of seventeen organizations, entities, or persons. There was a high level of concern. Fifty percent or more of the respondents indicated that they believed that each of the following entities could be the source of an invasion of privacy: a credit rating agency, a computer or data bank, an insurance company, the provincial or federal government, a bank, someone who could interfere with their mail, and someone telephoning them. Again, people who reported knowledge of microelectronic technology were those most likely to anticipate the likelihood of a privacy invasion.

A November 1982 survey conducted in London, Ontario by Professor Neil Vidmar of the University of Western Ontario[3] for the Ontario Government indicated similarly high levels of concern for privacy in the development of interactive services on cable television. Over two-thirds of those surveyed believe that Canadians have less privacy now than ten years ago. The types of information identified as most sensitive and most in need of protection were bank balances, information on when a person enters or leaves his or her home (information collected by home security systems delivered by cable), credit records, personal earnings and medical records. The findings showed that nearly half of the survey respondents were worried about government use of information, but an even greater proportion distrusted private business. Seventy-two percent of the sample favored regulatory intervention by government, with a majority of 52% seeing a regulatory role for both the federal and provincial governments. The study also indicated a widespread belief that many public and private organizations collect more personal information than is necessary.

Industry Response

As the OECD guidelines[4] have noted, one major means to effective privacy protection is the development of self-regulation by industries and firms which make extensive use of personal information. Several firms in this category have responded to the challenge of self-regulation with well developed internal practices, corresponding to the common definition of fair information practices outlined by the OECD, among others.

Bell Canada, for example, is a major corporation which handles a substantial amount of personal information which is necessarily collected for billing purposes. Company policies consider all subscriber information except name, address and telephone number to be private information held on a need-to- know basis within the company. Personal data are not available for sale, and Bell employees are instructed that all information about customers, wherever collected, is strictly confidential. Indeed the existence, content or nature of any customer communications are not to be made known to third parties, except in compliance with a legal order. Should such an order be made, Bell will notify the customer of the order unless specifically prohibited from doing so.

The Bank of Montreal is another personal data user which has developed and published information on its specific privacy protection practices. Data collected and maintained on file is the minimum necessary for the service desired. Access to that information is strictly controlled within the company, and information is generally not conveyed to third parties without the customer's consent, except that required by

statute or court order. Customer applications for credit card services, personal loans and mortgage loans, however, include a general consent or waiver clause which authorizes the bank to disclose information about the customer to third parties under certain circumstances. The practice of requiring customers to sign waivers, common among financial institutions, has been criticized in the past as undermining the customer's privacy protection.

Industry-wide self-regulation through establishment of a privacy code is currently being developed by the cable industry in Canada through its association, the Canadian Cable Television Association. A CCTA subcommittee, using the highly regarded Warner -Amex cable privacy code in the United States as a starting point, is in the process of creating a code for the industry tailored to the Canadian situation. It is expected that this code will be accepted and implemented by CCTA member companies as they develop their interactive service offerings. A major advantage of code development prior to the development of services is that systems can be designed in advance to enhance computer security and data protection capabilities.

Companies with voluntary privacy codes are still the exception rather than the norm, however. It is clear, therefore, that the widespread computerized handling of personal information will require the setting of standards in some form to ensure that infringement of citizens' privacy rights do not occur.

PART II: LEGISLATION GOVERNING PUBLIC SECTOR DATA BANKS

There is a growing body of legislation, in Canada and abroad, which addresses itself to the issues surrounding information access and privacy. That most of it is of fairly recent origin reveals the extent to which these issues are interconnected with developing information technologies and the speed with which privacy problems are expected to reach serious proportions. A variety of solutions are in evidence here, some dealing only with the question of privacy as affected by government data banks, others addressing the question of private sector data protection as well.

Canada

Privacy protection on the national level in Canada is focused on development of fair information practices in government data banks under federal jurisdiction. The Canadian Privacy Act, passed in 1982 and proclaimed in 1983, establishes the right of Canadian citizens and permanent residents to know, with certain exceptions, of the existence of information files on them; to examine, correct and challenge information in them; to know to what uses the file has been put; and to be consulted regarding certain future uses thereof. A companion statute, the Access to Information Act, was designed to maximize compatibility between information access and privacy. The Privacy Act requires publication of an annual index to federal information banks, and creates a Privacy Commissioner with the power to mediate disputes, investigate to ensure compliance by the data bank holder in question, and apply to the courts for review of government decisions to withhold information.

Provinces

Both Nova Scotia and New Brunswick have freedom of information legislation dating from the late 1970's. Nova Scotia's lists the types of documents that may be accessed, rather than establishing a general access principle, while the New Brunswick Act establishes general principles, with appeals to an ombudsman and in camera inspection by the courts of contested documents.

Newfoundland passed both Freedom of Information and Privacy Acts in 1981. The former lists the departments, boards, agencies and commissions affected, while the latter makes it "a tort, actionable

without proof of damage, for a person-...to violate the privacy of an individual."

Quebec deals with freedom of information and privacy together in an Act passed in 1982 and designed, like the federal Act, to protect personal information in government files, while allowing access to documents of public bodies. These bodies include not only the provincial government and all its departments and agencies, but also municipalities (including county, regional and city governments and agencies), and educational, health and social service institutions. The Act requires that an index of files kept by public bodies be compiled for circulation by The Information Access Commission and that requests for information be processed free of charge and within twenty days of receipt. The Commission has a variety of supervisory, investigatory and decision-making powers.

Ontario has examined the questions of privacy and access to information extensively in the past. As a result it has been proposed, in Ontario's Privacy and Access to Information Bill, that fair information practices be defined and made obligatory for government data banks. The proposal would establish a Data Protection Office with authority to develop and apply standards for the management of personal data systems. These standards would include requirements to restrict information collection to the minimum essential for the operation of a program; provide that personal information normally be collected directly from its subject, and that the reason for its collection be disclosed; and generally require that information collected not be disclosed without the individual's consent. Exceptions to the rule of authorized disclosure include occasions where it would not represent an unwarranted invasion of personal privacy, where it is necessary for the administration of authorized government programs, or where it is in the best interests of the individual or society. Individuals would also have the right to access and correction of files, with the data holder obligated to notify past users of the file of any correction. Individuals would also have the right to file complaints to a separate Commissioner's office.

In 1968 British Columbia passed the Privacy Act and became the first Commonwealth jurisdiction to establish an independent cause of action for the unreasonable and unwarranted invasion of an individual's privacy. This Act was followed by similar legislation in Manitoba and Saskatchewan. None of these privacy Acts, however, deal expressly with the inappropriate or unauthorized use of personal information which has been given voluntarily to another person or institution and integrated into an information bank. Moreover, there is a strong financial disincentive to the individual in enforcing his or her rights through the courts, since the costs of the action would often outweigh potential benefits.

United States

The United States' Privacy Act dates from 1974 and applies to personal information held in government records. It is essentially a "good housekeeping" statute which sets standards for administration of data files. As such, it requires government to report regarding the existence of information files, to ensure the quality of the information therein, to provide access to the subjects of such files, to use data only for the purposes for which it was collected, and to provide a record of disclosures of that information to the individual affected. There are no time limits for response, and the Act is self-enforcing in that the individual affected has recourse to the courts rather than a separate authority. The United States also has a Freedom of Information Act with rather wider rights of access than the Privacy Act.

United Kingdom

Parliament passed data protection legislation in 1984 which encompasses both private and public sector automated data banks. This legislation establishes a Data Protection Registrar

and Tribunal; requires that both private and public data banks be registered (with certain exceptions); prohibits unauthorized disclosure of information; provides access for individuals to data in registered data banks; and entitles them to amend files and to seek compensation in the courts for damages suffered. The Registrar is empowered to de-register data banks which contravene data protection principles and can prohibit the transfer of data outside the United Kingdom where the country of destination fails to meet minimum data protection standards. This legislation will enable the United Kingdom to adhere to the Council of Europe Convention on data protection.

Federal Republic of Germany

While there is no general access to information law, the Federal Republic of Germany has a highly developed network of data protection arrangements aimed at safeguarding personal privacy. These include both the Federal Data Protection Act and state data protection legislation, which enshrine in law the data protection principles of the Council of Europe. The Federal Act covers both federal public sector data banks and the private sector on a nationwide basis, while state Acts each govern their respective government's data practices. Primary responsibility for ensuring that the laws are followed falls on the heads of government agencies which create and use personal information files. As well, both federal and state legislation provide for the establishment of the office of Data Protection Commissioner, with responsibility to supervise and advise agencies which handle personal data and to report to the legislature annually. The success of this system of data protection lies not in the coercive powers available to the Data Commission, but on the high degree of consciousness of appropriate data handling procedures which has been achieved both in the public and in government.

Sweden

Sweden has been the world leader in both access to information and data protection legislation. Access to government information is regulated by the Freedom of the Press Act and the Secrecy Act, which taken together, provide access within a set of specific and limited exceptions. Information privacy is provided through several legislative Acts, the most important of which is the Data Act of 1973. This Act created a Data Inspection Board to regulate the collection and use of personal data in computerized form in both the public and private sectors. Thus the major function of the Board is the licensing of all data registers held by government or private sector data users, and the setting of the rules which govern their use. Decisions of the Board can be appealed to the Minister of Justice and to Cabinet, though the number of such appeals has consistently been small. In general, the first priority of the system is the protection of personal privacy, with less weight given to economy and efficiency in data use.

Council of Europe

The Council of Europe has prepared a "Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data" which has as its purpose the securing of respect for the individual's right to informational privacy. It requires signatory states to give effect in domestic law to the basic principles for data protection embodied in the Convention. These include: fair information gathering practices; limitations on use and contents of files in light of the purposes for which they were gathered; accuracy; minimal identification of individuals; limitations on the kinds of data to be processed; appropriate security measures; and procedures for identification, examination and correction of files by the individual to whom they pertain. It also confirms the right of signatory states to refuse to allow personal information to be sent to countries without comparable data protection provisions.

Organization for Economic Cooperation and Development (OECD)

The Council of the OECD has developed guidelines governing the protection of privacy, which it regards as minimum standards for its members. In a manner similar to the Convention of the Council of Europe, the OECD subscribes to the following principles: collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation and accountability. While specifically noting that data protection should not provide an excuse for restriction of transborder data flow, the OECD agrees that member countries should prevent the export of data which circumvents domestic privacy legislation, or involves export of data to countries not substantially observing the OECD principles. In particular, member countries are urged to: adopt appropriate domestic legislation; encourage and support self-regulation; provide reasonable means for individuals to exercise their rights; provide adequate sanctions; and ensure that there is no unfair discrimination against data subjects.

Summary

The preceding discussion suggests that the privacy legislation in these various jurisdictions covers a wide spectrum. Most laws ascribe to a similar set of fair information practices or principles. Although there is some variation on finer points, such as whether or not information collected must be "relevant" and collected "directly", most laws establish individual rights to access and correction, and build in some controls over the transfer of personal information to third parties. However, beyond this basic similarity, these laws vary greatly in their strength and application.

For the purposes of this paper, it is worth noting three of the models discussed above. The United States Privacy Act, at one end of the spectrum, provides an example of a self-enforcing law which sets out certain individual rights but does not establish a separate enforcement agency. The Act leaves it up to the individual to seek recourse through the courts.

A second model, illustrated by the Canadian Privacy Act, establishes an enforcement agency with investigation and monitoring responsibilities. Aggrieved individuals can complain to the Privacy Commissioner who can also apply to the courts for review of government decisions to withhold information. The new Quebec law has some similarities, although it has wider application, covering municipalities, school boards, universities and health and social service agencies as well as government departments. The Quebec law gives its Commission significant powers to supervise information practices, respond to complaints, conduct investigations, and issue binding orders to a public body.

A third model that could be identified on this spectrum is illustrated by the United Kingdom registration system described above. In some ways this system of regulation is stronger than the two models summarized above because it requires the formal registration of data banks and gives the Registrar substantial powers of investigation and enforcement, including the power to refuse registration of data banks if the user does not comply with the principles of the Act. The Swedish and German registration systems go further and could be regarded as two additional models on this spectrum.

PART III: ALTERNATIVES FOR THE PRIVATE SECTOR

Summary of Issues

The first part of this paper has discussed the challenge which computerized handling of personal information poses for the protection of privacy. From this discussion emerge a number of competing notions. Most would agree that there is a need to weigh the gains in computer efficiency and speed against the costs to individual privacy which have arisen. In economic terms, therefore, there are conflicting pressures

for business establishments to achieve all the cost savings new technology has to offer on the one hand, and to provide the individual with reasonable privacy protection, on the other.

Although it is difficult to generalize, the cost of providing minimum privacy protection is thought not to be great in relation to the efficiency savings usually afforded by new technology. Moreover, these "protection" costs are often minimized if standards or procedures are established prior to the introduction of new systems.

The privacy issues outlined in Part I could be summarized as follows:

1) Data Collection: Should personal information collected by data users[5] be limited to that which is relevant to the user's specified purpose and to that which has received the data subject's informed consent? Should there be a further requirement that personal information be collected directly from the data subject? The major statements of principle on the data collection issue usually also include a reference to data being obtained fairly and lawfully for a legitimate purpose. This paper assumes that legitimacy is not at issue and will focus on relevance and informed consent with regard to data collection.

2) Data Quality: Should personal information collected by data users be subject to a requirement to be accurate, complete and up-to-date?

3) Disclosure Limitations: Should disclosure of personal information by data users to third parties be limited to only that information required to fulfill the user's specified purpose? Exceptions would include cases where the subject consents or where disclosure is compelled by law.

4) Security Safeguards: Should data users be subject to a requirement to ensure the physical security of personal records?

5) Individual Access: Should data subjects have the right to confirm the existence of their personal data in records, inspect and receive copies of the data, and request changes to erroneous or incomplete data?

6) Costs: If citizens are given rights of access, correction and non-disclosure, the cost of enforcing these rights must not be prohibitive. Regulatory options which give enforcement agencies quasi-judicial powers to settle grievances may present one option for providing enforceable rights for individuals.

This section will analyze a number of alternative solutions to these issues as they apply to the private sector and then review the strengths and weaknesses of each alternative. The analysis begins with the assumption that the need for informational privacy is a legitimate claim and that the principles enunciated by the Council of Europe's Convention on Data Protection (summarized on page 4) represent a reasonable list with which to evaluate policy alternatives in this area.

Scope

This paper attempts to deal with both the public and private sectors. From the individual citizen's point of view, the threat to privacy of personal information exists in both sectors. Although North American privacy laws have thus far only addressed the problem in the public sector, countries like the United Kingdom[6], West Germany and Sweden have legislative programs in place which cover both sectors.

This leads to the question of self-regulation or government regulation. Some of the competing arguments concerning the effectiveness and desirability of self-regulation as a means of ensuring fair information practices will be examined below in the context of the private sector.

Another general question which all jurisdictions have to decide is whether regulatory programs should cover only computerized personal records or whether they should apply to all personal records, manual and computerized. The major premise in the United Kingdom's White Paper on data protection is that computerization presents new threats to privacy because of the speed, low cost and ease with which personal information can now be distributed. The implication here is that the costs and effort involved in the transferring of information in manual files act as a disincentive to unauthorized disclosure.

On the other hand, the data protection laws covering public sector records in North American jurisdictions do not distinguish between computerized and manual records. These laws provide the individual with certain rights regarding personal information in both computerized and manual records. The importance of manual records is seen when categories such as health information are considered.

Another important question is whether all data banks, or only those above a threshold size, should be covered by whatever regulatory or self-regulatory approach is undertaken. It is argued by some that only those data users above a threshold size should be candidates for regulation, since the cost of compliance is a greater burden for smaller institutions. However, exemption of smaller data banks would leave information in those banks unprotected, thereby weakening individual rights.

Policy Options

This section looks at four possible options: a voluntary privacy code, a legislated code, a registration and regulation system, as well as an approach which combines elements of the first three. This list is not intended to be exhaustive, but to offer for discussion some reasonable alternatives which could fit the Canadian situation.

1) Voluntary Privacy Code: If the need for privacy protection is accepted as a legitimate claim, governments could encourage specific industries (through their associations) and corporations which are important data users to develop voluntary codes, incorporating the important principles normally embodied in data protection laws. Companies such as Warner-Amex in the U.S. and IBM in Europe have already developed guidelines for the protection of personal information in their files. In Canada, the Canadian Cable Television Association is in the process of developing a privacy code.

In 1981, Warner-Amex Cable Communications Inc. developed a code designed to protect the privacy of personal information which the company compiles on individual subscribers of cable TV services. In the code, the Company agrees to keep subscriber information physically secure and confidential and agrees to keep subscribers informed of all information gathering functions of the cable TV services being provided. Agreements with individual subscribers set out the terms under which information will be used and provide that no other individual data will be collected without the individual's consent. The code also gives the subscriber the right to examine his or her file and request corrections of erroneous data.

The code is being made a part of subscriber contracts and franchise agreements, making it self-enforcing and giving the subscriber certain rights by agreement. In theory, an individual who felt that his privacy rights had been infringed could commence a civil legal action for breach of contract.

Comments: The advantages and disadvantages of the voluntary code approach as a resolution to privacy issues could be summarized as follows:

- It provides no assurance that the majority of important data users will voluntarily adopt codes.
- No formal enforcement or compliance methods are established (except the limited power of the individual to seek recourse for breach of contract, in cases where the code is

supplemented by a written agreement between data user and subject).

- It imposes the least cost and interference on data users.
- It features maximum flexibility, since codes could adapt to changing technology and public requirements.
- It does not guarantee substantial rights for individuals in the case of a dispute over access, correction or disclosure.
- The adoption of various voluntary codes by different industry sectors and companies would result in a lack of uniformity of privacy protection for individuals.

2) Legislated Privacy Code: One approach which falls in between voluntary codes and more traditional government regulatory solutions, consists of developing legislation which would set out fair information practices and would include a penalty provision for the offense of violating these practices. Fair information practices could cover the issues of data collection and quality, disclosure limitations, security safeguards and individual access as set out above. This law would permit a civil lawsuit in tort and would essentially constitute a self-regulatory approach to the problem since it would not require the establishment of an enforcement agency.

Some authors have suggested that public demands for privacy rights have arisen from the failure of legislatures and courts to develop such a body of law[8]. It is generally agreed that the common law in Commonwealth countries offers no protection for personal privacy *per se*.

The Privacy Acts enacted by British Columbia, Saskatchewan and Manitoba have been used infrequently and are also thought not to provide the individual with substantial remedies for the types of privacy problems brought on by the computerized handling of personal information.

Legislation establishing a privacy code could take one of two forms:

(a) An Act could permit voluntary compliance. Regulations to the Act could register those industries or companies which wish to comply. Voluntary participants would thus be identified as privacy-conscious companies in their field.

(b) Alternatively, an Act could require compliance. It could apply to all data users, or only to those institutions with data banks above a threshold size.

Comments: Following is a summary of the strengths and weaknesses of this approach:

- It provides no assurance that a majority of data users would voluntarily comply. Only the compulsory version of such a statute would guarantee participation by a majority of data users.
- The remedy available to the individual is costly and impractical. It would likely not be used often since the cost to the individual would almost always exceed possible benefits from using this remedy. Therefore, this approach also does not provide substantial rights to individuals regarding access, correction, disclosure and resolution of disputes.
- It imposes little cost and interference on data users.
- It allows a high degree of flexibility, since the legislation would phrase fair information practices in general terms, thereby not hampering the application of new technology.
- If remedies were not used widely by individuals, such an Act would not have a major effect on information practices. The compulsory version of such an Act, however, might encourage some uniformity in general data collection and disclosure practices.

3. Registration and Regulation: Another possible solution to these issues is for government to legislate to require registration of data banks; give individuals defined rights of access and correction; regulate the collection and third-party

disclosure of personal information; guarantee the security of data and establish a Registrar with investigation and enforcement responsibilities. The registration requirement could apply to those institutions which automatically process personal information in data banks.

This is basically the approach taken by the United Kingdom in their Data Protection Bill, referred to in Part II of this paper. This Bill sets out a registration and enforcement system covering data users which process personal information automatically. Although it applies to both the public and private sectors, the basic structure of this registration system can serve as a useful model for our discussion purposes here.

In this model, the public registry of data users helps individuals become aware of the existence and purpose of computerized personal information banks. The data user is required to identify himself, the information he uses, where it has come from and to whom it is disclosed, as well as the purposes for which it is used. The Registrar has the power to make inquires, to inspect data files and to require modifications to a system. In extreme cases, he may refuse registration for non-compliance with the major data protection principles embodied in the Act. Since the Registrar is given such wide powers, the Bill sets up an appeal process to an independent tribunal, composed of judicial and computer experts.

The United Kingdom Bill also gives the individual rights of access to personal data; the right to compensation for damages from use of inaccurate data, loss of data and unauthorized disclosure; as well as the right to apply to the courts for rectification or erasure of incorrect data. The individual would have to apply to the court if a data user contravenes any of these individual rights, in order to secure compliance or seek damages in civil proceedings.

Other features of the Bill enable the Government to restrict the transfer of categories of information to specified countries which do not have data protection legislation of comparable strength; give the power to make regulations governing particular categories of personal data such as racial origin, political and religious beliefs; and exempt the collection of data for research purposes where individuals are not identifiable.

The following comments focus only on the general characteristics of a registration system such as the one modeled in the United Kingdom Bill as they could apply to the private sector. They are not meant as an evaluation of the Bill overall.

Comments: The advantages and disadvantages of this approach could be summarized as follows:

- It provides legislated privacy protection covering all important data users and includes an enforcement mechanism to ensure compliance.
- It provides the individual with legal rights of access and correction as well as protection against disclosure to third parties. However, the enforcement of these rights in the case of a dispute may be costly to the individual if the remedy involves application to the courts.
- This approach imposes new regulation on the private sector, resulting in additional costs for data users.
- It allows some flexibility, since the data protection principles are general and the Registrar's powers are defined broadly, allowing him to handle demands of changing technology and information practices.
- It would have a major impact on information practices because of the registration and enforcement powers.

Registration schemes are a common feature of data protection legislation in other European countries. Brief descriptions of the legislation in West Germany and Sweden, probably the other two most noteworthy examples, are given in Part II.

Many Canadian provinces regulate the collection and disclosure of personal credit information through credit reporting Acts. In Ontario, for example, the Consumer Reporting Act registers Consumer reporting agencies, regulates the gathering, storage and disclosure of credit information, and gives the individual access to his or her personal credit file. The Registrar has the power to revoke or refuse registration under certain circumstances, in which case the applicant is entitled to an appeal to a tribunal. The models used by provinces to regulate credit information might also provide some guidance to registration systems contemplated for personal data users.

4. Voluntary Registration: Combinations of the above three approaches could produce other possibilities. One such possibility which is worthy of analysis is a combination of the Self-Regulation and Registration approaches described above. Industry associations could develop privacy codes tailored to their industry, monitor compliance among their members, and mediate complaints from individual citizens. This could be done in consultation with a public Privacy Office which could also keep a registry of all participating associations and companies.

Comments: Following is a summary of the strengths and weaknesses of this approach:

- As in the self-regulation model, this solution offers no assurance that the majority of data users will voluntarily join a registration system.
- It would establish a monitoring system to encourage compliance by participating companies and agencies. Although this could be a very positive force, no formal compliance or enforcement powers would be available.
- It would result in some extra costs to data users.
- It features a great degree of flexibility allowing industry and the coordinating agency to respond to changing technology and information practices.
- It does not guarantee concrete rights for individuals in the case of a dispute over access, correction or disclosure. The complaint handling activities of industry associations, however, could fulfill a mediation role.
- Although the adoption of different privacy codes by different industry sectors would result in some differences in privacy standards across the economy, the coordinating agency could work for uniformity on important issues such as the individual's rights to access, correction and non-disclosure.

Summary

This section has attempted to compare the effectiveness of several alternative methods of resolving informational privacy issues in the private sector. Rather than reviewing all the possible approaches, including more stringent government registration and licencing schemes, this paper has focused on those approaches which are thought to be more suitable to the Canadian situation.

The table on the following page contains a comparative summary of the four approaches outlined above. The criteria used for comparison are based on the preceding analysis and reflect the major consideration central to any discussion of regulatory options: the balance between cost to industry and the provision of individual rights or protections to citizens. Terms in the table, such as "Low/Medium/High" are used to suggest relative values only.

Footnotes:

1. See Ontario Consumer Issues 1980 and Ontario Consumer Issues 1983, Ontario Ministry of Consumer and Commercial Relations.

2. A Gallup Survey of Electronic Technology, March 1981, The Gallup Organization, Inc.

3. Neil Vidmar, Privacy and Two-Way Cable Television: A Study of Canadian Public Opinion, University of Western Ontario, 1983.

4. Organization for Economic Cooperation and Development, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.

5. The following definitions are used in this section:

Data User: Institution which collects and handles personal information on individuals. Data Subject: Individual who is the subject of data collection.

6. Data Protection Act, 1984

7. Data Protection: The Government's Proposals for Legislation, Home Office, United Kingdom, April 1982.

8. For example, see Roger Noll, "Regulation and Computer Services", in M. Dertouzos and J. Moses, The Computer Age: A Twenty-Year Review, (Cambridge: MIT Press, 1980) and Murray Rankin, Privacy and Technology: A Canadian Perspective (Canadian Institute for Legal Studies, Cambridge University, 1983).

EVALUATION OF ALTERNATIVE SOLUTIONS

	ALTERNATIVES			
BASIC CRITERIA	VOLUNTARY PRIVACY CODES	LEGISLATED PRIVACY CODES	REGISTRATION AND REGULATION	VOLUNTARY REGISTRATION
Cost of Compliance to Data User	Minimum	Minimum	Moderate to High	Moderate
Flexibility	Maximum	Moderate	Moderate	Maximum
Individual Rights to Access, Correction and Non-Disclosure	No Guarantee	Legislated rights under compulsory version of such a law	Establishes Legal Rights for Individuals	No Guarantee
Individual Rights in Dispute Resolution	None	Costly and difficult for individual to enforce	Through the Courts; Appeal to Registrar Provides Alternative	None
Uniformity of Information Practices	Difficult to Achieve	Possible under compulsory version of such a law	Registration Encourages Uniformity	Some Uniformity Possible
Effectiveness in Developing Overall Standards for Privacy	Low to Medium	Low to Medium	High Potential	Medium

PART B

MAJOR CONFERENCE ADDRESSES

KEYNOTE SPEECH ON PRIVACY: INITIATIVES FOR 1984

THE HONOURABLE NORMAN W. STERLING, Q.C. *
Provincial Secretary for
Resources Development, Ontario

Good Morning,

It certainly is a pleasure to welcome you to the first Inter-Provincial Conference on computers and privacy. It is long overdue. I say the first, because I believe this conference is unique in that we will be exploring issues and options which have never been discussed in a forum such as this before.

Indeed the overwhelming response which we have received for this symposium is most encouraging. In fact, close to 300 members of the industrial, medical and business communities are represented here today. This indicates to me that not only are businesses and governments concerned with the problem, but that this collective involvement also signals the need for us as a nation, to develop a uniform approach to the privacy problem.

In recent years the issues surrounding privacy have been greatly accelerated by rapidly changing and increasingly sophisticated technology systems.

The attendance here today is evidence that we are all affected: governments, consumers, bankers, medical practitioners, and small and large businesses alike.

You know, it is somewhat ironic that although we as citizens view privacy as something precious - something which we cherish and guard closely - there has never been adequate legal recognition or proper safeguards to ensure this right.

Oh, I'm aware that there are some limited privacy Acts in existence; and that the Federal Government has proposed changes to the Criminal Code which will specifically address computer crime. But it is important to remember that these changes will only address the blatant abuses of security - the horror stories which we occasionally read about in the papers.

For example, one of the most extreme cases of abuse which I have heard recently involved a young man who was able to use his home computer to gain access, and consequently change the billing structure of over 6,000 radiation therapy records of patients at a cancer centre in Manhattan.

In one respect, this incursion into privacy is alarming. Yet, because the example illustrates such a blatant breach of security, it will, in many respects, be much easier for legislators to address. The criminal code amendments are however only a very small step.

---

* Mr. Sterling, who is the MPP for Carleton-Grenville, Ontario, is a graduate of Carleton University, Bachelor of Engineering (Civil). He is also a graduate of the Faculty of Law, University of Ottawa (1969). He was first elected to the Legislature in 1977and appointed Minister without Portfolio April 10, 1981. He was appointed Provincial Secretary for Justice on February 3, 1982 and Provincial Secretary for Resources Development on July 6, 1983. He is the Ontario Minister responsible for privacy and access to information laws.

The larger, much broader issue at stake is the current free-wheeling exchange and selling of information via electronic means which poses perhaps the greatest challenge to privacy.

Unfortunately, the Canadian emphasis appears to be on modifying existing legislation. I believe, however, that that is simply not enough. It is now necessary to look at developing standards that will deal directly with the much more subtle and broader problem of data control.

While I do not wish to over-dramatize the situation, I think Ralph Nader put it well when he said in 1971: "It is a rare American who does not live in the shadow of his dossier... What the misuse of computers is doing and can do to an individual's freedom (constitutes) a warning of a new form of slavery."

Clearly, this Orwellian vision has not become the reality which Nader states.

On the other hand what has occurred is much more subtle, yet nonetheless equally important. At present, there is no recourse for the individual who feels that the information he has supplied has been used without his authorization. In that sense, perhaps we have become slaves to technology.

When an individual provides information he does so for a specific purpose. He does not do it with the knowledge that the course for this information has only begun what is probably a long journey into a nebulous state of free-flowing data.

To illustrate my point, I will refer to the somewhat simplistic yet compelling case of subscriber lists. I am sure everyone here can relate to what happens should you decide to subscribe to a particular service. Before you know it, you find you are receiving an extraordinary amount of "invitations" to join every other service, which may or may not be even remotely related to the original subscription. Chances are, you are annoyed - but what can you do? Your privacy, although invaded, has not caused any direct harm.

So you toss the "Invitations" and continue with your daily life.

The nagging question though - which never seems to be answered is: How did "those" people get my name, and address? How do "they" know my personal preferences? What else do "they" know? What else are "they" capable of finding out? and most important, How do I stop this? Who do I complain to?

I do not believe that industry's motives are sinister. Rather I believe that most companies handle consumer information in a responsible manner. The primary motive is quite simply one of economics. There is a great deal of money to be gained from the selling of information. And, there isn't anything inherently wrong with that motive in isolation.

The point I wish to stress is not the fact that the information is sold. That is only the tip of the iceberg. Rather, it is the end result which has inadvertently produced a matter of great concern - namely, a citizen's right to privacy.

The complexity of this issue is compounded when the information begins to cross borders, whether they be provincial or international. Commonly referred to as transborder data flow - the emphasis should be placed on the word "border". The current electronic age which we all find ourselves in is making those borders increasingly fluid. The lines are no longer distinct; they have become blurred.

This blurriness has made it impossible for any one jurisdiction to address the privacy issue in isolation. The necessity for a coordinated and comparable approach has been recognized by the Council of Europe.

In 1981, in Strasbourg, France, the Council adopted a Data Protection Convention. The recommendations were signed by 16 participating countries.

When this convention comes into force it will confirm the right of countries with data protection legislation to refuse to allow personal information to be sent to

other countries which do not have comparable safeguards. This could threaten industries with international interests operating in one country, but which process data for customers in many different nations.

At present, four countries - Sweden, France, Spain and Norway-have ratified the convention. In other words, they have not merely signed it, but have enacted legislation. In addition, the United Kingdom has formally stated its intention to ratify, as soon as the Data Protection Bill is passed by Parliament. The Bill which received 2nd reading last March is expected to be passed this summer. A total of five countries are required before the articles of the Convention can take effect.

The legislation proposed by the United Kingdom is interesting in that it encompasses both the private and public sectors. The central feature behind this initiative is the establishment of a Data Protection Registrar and Tribunal. In this respect all users of electronic data systems, with some exceptions, must register. The Registrar would be empowered to examine alleged cases of misuse and subsequently "de-register" data banks which contravene data protection principles.

As well, the Data Protection Registrar can prohibit the transfer of data outside the United Kingdom where the country of destination fails to meet minimum data protection standards. The direct implications of this last point could indeed be tremendous for Canadian companies who do business with the United Kingdom. To illustrate the potential impact, in Ontario, nearly 20 percent of our work force -- more than 800,000 people -- depend on export-related activities for their jobs. In 1982, 40% of the Ontario jobs in the manufacturing sector depended on sales outside Canada.

The hard fact ladies and gentlemen is that unless we develop guidelines governing data protection, future trade discussions could indeed be affected.

To sum up, the issues we will be discussing during the next two days are far-reaching. For the matter of privacy has, in effect, also become a matter of economy. As governments, we must address the concerns surrounding the protection of individual privacy and general access rights.

For industry, it becomes a bit of a juggling act: these same concerns must be further balanced against a need for information, in conjunction with the cost of implementing privacy safeguards.

In Ontario we have examined the questions of privacy vs access and have tried to strike the difficult yet vital balance between the two in the public sector.

Ontario's proposed privacy and access legislation is focussed on the development of fair information practices for government data banks. The establishment of a Privacy and Information Commissioner will provide citizens with an appeal mechanism concerning the release or protection of documents.

In addition, the formation of a Data Protection Office is also proposed in the Bill. The principal thrust and mandate behind this new initiative will be to provide internal guidelines and to act as a privacy "watch dog" within government.

So, what then are the options for Canada? Enclosed in the Conference Kit is a Discussion Paper on Privacy.

Essentially, the Paper examines options and possible initiatives which could be introduced by both the public and private sectors.

There are four possible routes which we can explore. One, a voluntary privacy code, which I just referred to; two, a legislated privacy code; three, a system of registration and regulation; and four, an approach which combines elements of the first three.

This list is clearly not an exhaustive one. But I suspect that it does offer some "food for thought" and will provide for considerable discussion during the next two days.

From the individual citizen's point of view, the threat to privacy of personal information exists in both sectors. Thus far, however, North American privacy laws have only addressed the issue in the public sector.

The need to broaden the scope and to establish standards becomes readily apparent when one sees that companies with voluntary privacy codes are still the exception rather than the rule. It is clear that the increasing and widespread use of computerized information requires some safeguards. These safeguards must ensure that an individual's right to privacy is not infringed upon.

The voluntary code allows industry maximum flexibility towards the incorporation of data protection standards. It would also be adaptable to changing techology and public requirements. Companies such as Warner Amex Cable in the U.S., and IBM in Europe have already developed guidelines for the protection of personal information in their files. In Canada, it is my understanding that the Canadian Cable Television Association is in the process of developing a privacy code.

While such responsible corporate action is commendable, a uniform approach may be necessary to address privacy problems. Clearly the adoption of various voluntary codes, by different sectors, could result in a patch-work approach.

A compromise between the voluntary code and the more traditional government regulatory solutions lies in the legislative route. In essense, a government could set out fair information practices which would also include a sanction for the violation of those practices. This law would essentially allow for self regulation of industry and would permit legal remedy.

While this option does contain some benefits, it does not really provide a practical solution. Realistically speaking, I don't think many individuals would undertake the time and cost that is involved in pursuit of a civil lawsuit.

On the other side of the coin exists the option of complete registration and regulation. This basically is the approach which has been taken in the United Kingdom Data Protection Bill. Essentially, government would be empowered to: give individuals defined rights to access and correction; regulate the collection and third party disclosure of personal information; and guarantee the security of data by establishing a registrar with investigation and enforcement responsibilities. In short, the collection of personal information in an electronic data bank becomes a privilege and not a right.

The fourth approach is a combination of the three I have just discussed. Essentially it involves a combination of self registration and regulation.

Associations would be encourage to develop privacy codes tailored to their industry. An internal monitoring system would be a very positive force towards ensuring compliance among industry. In cooperation with a public Privacy Office, a registry could be maintained of all participating associations and companies.

I think it is important to stress that governments must not over-react. Industry must be allowed the opportunity to respond to these new challenges in a reasonable and responsible manner. Before we all embark on an "Anti '1984' crusade", let's examine the alternatives closely.

I am confident that given the opportunity and the interest shown here today, by both the public and private sectors, we will be able to further our dialogue in a meaningful and constructive fashion.

Thank you.

PROTECTION OF PERSONAL INFORMATION IN THE U.K.:

THE DATA PROTECTION BILL

THE HONOURABLE DAVID WADDINGTON, Q.C. *
Minister of State for
The Home Office, United Kingdom

Mr. Sterling, when I was in the Department of Employment, where I was a Minister before being moved to the Home Office, I was minding my own business one morning and a secretary came in and said the Secretary of State is ill, here's a speech which he was going to make in the City of London, go off and make it and as I was in the car reading the speech feverishly, I said aloud, this is the dullest speech I've ever read and my secretary said, don't worry, Ministers are supposed to make dull speeches. Well, I shall try not to be too dull today.

I must tell you that when I went into the Home Office, not actually in January this year but in January of 1983, I knew that I was going to have to grapple with the problems of immigration and nationality, but I didn't really know what was coming to me. I certainly knew nothing whatsoever about privacy and data protection. I've now lived with the subject for a year and a half, I'm still learning, and one thing I've learned in Canada, is that in many respects you've got more experience in this field than ourselves, but I think that there is value to be gained from sharing experiences, so here goes.

I must be careful that we're more than usually careful, not to be divided by our common language and I better say a word or two about terminology. It's been brought home to me in the last 48 hours that many people here look upon freedom of information and privacy as part and parcel of the same problem, or the two sides of the same coin. We don't look at it in that way.

When we talk about the possibility of our passing a freedom of information bill through Parliament, we mean a bill which would reflect the commonly held view that there are certain activities of government, at present kept secret, which ought to be in the public domain.

When, on the other hand, we talk of privacy, we're expressing the notion that there is a part of the ordinary citizen's life which is peculiarly his own and should be free from outside interference or unwanted publicity.

Now we in Britain have always shied away from legislating for a general right of privacy. Privacy means different things to different people and, quite frankly, we take the view that if we were to establish a general right to privacy, nobody would have the faintest idea how the courts would handle the matter and what they would find to be a breach of the right of privacy and what they'd not find to be a breach of the right of privacy.

But what we have come to accept is the need for legislation in respect of one specific aspect of privacy and what now concerns an increasing number of people in the U.K. as elsewhere, is the particular threat to individual privacy

---

* Mr. Waddington, M.P. (Ribble Valley), is the Minister of State for Home Affairs, United Kingdom, responsible for immigration, nationality, community relations, voluntary services and data protection. He was responsible for steering the Data Protection Bill through Parliament.

posed as a result of information being held about individuals on computer, so very near to the end of its passage through Parliament, is what we call our Data Protection Bill.

It's not a very elegant name for a bill, but the term data protection has been in use in Europe for a long time now, so it really wasn't sensible to depart from that terminology, and call our bill, for instance, a Privacy Bill, but it is a Privacy Bill, it is not a Freedom of Information Bill.

Now, our bill differs greatly from your Federal Privacy Act. In one key respect, it does far less to enlarge the rights of the individual citizen, because it does not apply to information held about him, but only automatically processed data, i.e., personal information held on computer, but in another respect, as you'll all now know, it goes much further than your act because it covers the private, as well as the public sector and I should be talking a little about that later.

Now to make our approach begin to make sense, one has to go over a bit of history. Partly in response to the fears expressed by people about the possible threat to privacy posed by computers, in 1970, the Labour Government of the day set up a committee called the Younger Committee, named after a former Minister in a previous Labour Government and that Committee had a mandate to consider whether legislation was needed to provide protection against intrusions into privacy. The Younger Committee reported in 1972, and amongst other things, it recommended that computer users should voluntarily observe certain principles of information handling, and that the Government should legislate to set up a standing committee to keep the observance of the principles and the use of computers under review and make proposals for further legislation.

Well ladies and gentlemen, we've got many virtues as a nation, but we don't go in very often for sudden bursts of activity following the publication of the reports of committees, and I understand that that is sometimes something we share with you. By the time the Younger Committee reported, a Conservative Government was in power, and our Conservative Government, perhaps unlike your Conservative Governments, are perhaps even more reluctant to act on the recommendations of committees so nothing whatsoever happened. In 1974, the Labour Government won the election, and we were all keyed up for dramatic action but nothing followed - not for two or three years - and then what did they do, they set up a committee.

They set up the Lindop Committee which did not report until 1978 and in 1979 defeat at the polls relieved Labour of the whole problem, some hope for all time. Now that might have been the end of the story. The by-partisan policy of masterly inactivity could have continued for a very long time and certainly seen out my time in Parliament, which might have been better for my career, but some of us haven't reckoned with the goings on of our friends in Europe.

In Europe, the tradition of remitting difficult decisions to sedate committees isn't as refined, as advanced as in Britain, and legislation had already been passed in a number of places.

Now the front runner was the West German Province of Hess, and Hess legislated on this matter as long ago as 1970. Sweden followed suit in 1973, and by the end of the seventies, Germany, France, Norway, Denmark, Austria, Luxemburg, and Iceland, all had their data protection bills, all different from each other I might say, but all bills dealing with this field of personal information stored on computer.

Most important of all, a multi-national initiative had taken place in 1981. The Council of Europe had produced a convention, a convention which set out certain principles for data protection that users of computerized information should observe and which enjoined member states to pass national legislation to give effect to those principles.

The position is that now four states have ratified the European convention. The convention says that it comes into operation when fives states have ratified and therefore, no state can afford not to be looking very carefully now at its own position. Why? Because while the convention prohibits ratifying countries from in any way interfering with flows of data to other ratifying countries, a ratifying country can prohibit the export of personal data to a country which has not ratified.

So, it may interest you to know ladies and gentlemen, that unlike what I understand to be the position in Canada, we, after 1981, were faced with pressure to legislate, not just from those concerned about civil liberties and privacy, but also from a sizable chunk of industry concerned that Britain might find itself the odd man out in Europe, and that flows of data to and from Britain could be interrupted because of fears in another country that we did not provide adequate safeguards for the data. So there is one dramatic difference, as I understand it, between your situation and ours.

The result was obvious. A decision to legislate, not for all personal information, but, where the perceived threat to privacy was the greatest, and where the convention obliged us to legislate in the field of what the convention refers to as automated personal data files.

Now I'm sure I'm right when I talk about the perceived threat being computers. Of course, manually stored information can be misused, but the public concern, certainly in Britain, is and always has been focussed on computers and I can give a very good example of that.

Last year our Department of Health and Social Security decided to issue people with computer-readable plastic national insurance cards in replacement of the old cardboard cards. The same information was to appear on the new card as the old, just the individual's national insurance number, the purpose for which it was to be used was identical so that the individual could give a number when making his claim, but the result of that announced change was uproar.

Uproar because the public realized that machine-readability meant that in theory the information on the card could be transferred to others in the twinkling of an eye and then linked with other computerized information, even though in practice there were going to be no changes at all in the use of the information.

Now, of course, ladies and gentlemen, there was another reason why we never thought of extending the legislation to manually stored information - sheer practicality.

No doubt, I will hear from some of you afterwards what I think of the practicality of our legislation which covers almost everybody in the private sector, but certainly we thought that the prospect of extending this form of legislation to every box file in the country, was something to make the imagination boggle and we certainly weren't prepared to countenance it. In our minds that would be the road to a massive bureaucracy and a horrendous expense.

But even if the convention has not required us to cover the private sector, in the field of personal information on data files, we might have grappled with that mettle. I agree with the implicit assumption in provincial and federal legislation in Canada that the main concern, and the principle target, is government.

In my experience certainly when people talk of their privacy being threatened, they normally are talking of their privacy being threatened by government, but so long as one is talking about privacy, and not freedom of information, the legislation logically cannot be restricted to government.

One only has to think of the information that exists on employers' staff records, to appreciate how much harm may be done by inaccuracies or misleading statements, or by damaging disclosures of that information to others.

But what, Mr. Sterling, was to be the form of this legislation to cover only information on computer, but both the private and the public sector? We wanted data users to discipline themselves, but we did think that it was essential that the new obligations which we believed data users had to face, had to be brought home to them, that there was a lot of educating to be done, and that the best way to do this was through a system of registration, so registration it is.

Registration is a feature of most European data protection schemes and will force data users, large and small, public and private, to lodge particulars of their operations on a central register.

Under the bill, they have in registering to describe the personal data they hold (it only applies this obligation to personal data) and the requirement to register is a requirement to be imposed only on data users who are storing personal information, but they have in registering to describe the personal data they hold, the purposes for which they hold them, the sources of the data, and to whom they disclose the data.

It's important to note that that will involve them in a deal of self-scrutiny. It will make them consider what computer systems they actually possess, what data they hold there, and whether their uses of data match up to the general standards prescribed by the bill and, in addition, of course, the publication of a public register will bring out into the open what users are doing with the personal information they hold.

And, what are the standards data users will have to observe? Well, the convention contains certain principles to be observed, principles that were, in turn, drawn from the Younger Report and which have now, if I may use the expression, been repatriated to Britain.

We've won back the principles which actually were formulated by Younger.

We haven't just translated those principles into legally enforceable obligations, they are not specific enough, they're too generalized for that, but we have nonetheless embodied them in our legislation and there is going to be a data protection registrar, not dissimilar to your own privacy commissioner, to supervise their observance.

The result will be that if any data user contravenes any principle, the registrar will have power to take action against him, and can order him to take whatever steps may be necessary to come into compliance with that principle, including erasing the offending data.

It is then made an offence for a user not to comply with the registrar's order and right at the end of the line there is the power in the hands of the registrar to say to a data user who won't obey his order, right, I'm going to serve on you a de-registration notice, which means that thereafter it will be illegal for you to carry on your operations.

The principles are worth spelling out. First, the data should be obtained fairly and lawfully, thus if in the registrar's view data has been obtained by unfair means, perhaps somebody has been misled as to the purpose for which they will be held, the user will be in breach of the principles and may be ordered to erase the data.

Two, the data should be held only for specific, specified and lawful purposes, purposes specified in those registration particulars to which I referred. Third, the data shall not be used other than for those purposes specified in the registration particulars. Four, and here we come to the nature of the data themselves, the data held for any purpose shall be adequate, relevant and not excessive in relation to that purpose.

Five, they shall be accurate, and where necessary, kept up to date. Six, they shall not be kept for longer than is necessary for the purpose to which they are held.

The seventh principle deals with the matter of subject access. Individuals

are entitled to know whether data are held about them, to keep a copy of the data, and where any of the other principles has not been conformed with to have data corrected or erased.

And finally, the eighth principle, deals with security. It provides that appropriate security measures should be taken in respect of data held so a persons' privacy is not imperilled because of the slackness of the operations of the data user and unauthorized persons getting access to it.

What is perhaps worth emphasizing, is that in the generality of cases an individual will get the remedy he wants by going to the registrar, and he will not, under our scheme, have to go to the trouble and expense of bringing an action in the courts.

On the other hand, in certain respects the citizen will have a dual remedy. He can go to court for instance, for rectification or erasure of inaccurate data, or when he has been refused access to data, but those are both situations when he could, in any event, have gone to the registrar and said that this data user is holding inaccurate information about him.

I should mention one specific power of the registrar in view of what is going to happen in the next session of the conference. The registrar has power to step in where exports of data are concerned, transborder data flows, or TBDF in the jargon.

He can prohibit transfers of data to countries that have not ratified the convention if, and this is important, but only if, in his view the transfer will lead to any contravention of the principles. So we've armed our registrar with direct enforcement powers, his decisions are appealable to a special judicial tribunal, but if they are upheld by the tribunal, it will be an offence to defy them.

He is an enforcement agency with very real powers, he'll be wholly independent of government, he'll be appointed by the Queen by Letters Patent, he will set up his own office and employ his own staff. The size of the staff? We envisage only twenty to thirty. We've no intention of giving birth to a vast bureaucracy, we want the system to be effective but to do its job without undue cost to industry. We've been conscious the whole time of the need to strike a reasonable balance between the rights of the data subject on the one hand, and the rights of the data user on the other, recognizing that the imposition of excessive costs on industry could lead to new costs on society as a whole, in terms for instance, of more unemployment. We are determined that registration should be a simple process costing only a few pounds a year.

We also hope that it will be possible to set a charge for subject access, which will in the vast majority of cases, cover the cost of business of granting access, but we will always have to bear in mind the requirement of the convention that subject access must be granted "without excessive expense".

Businessmen please note the following:

(1) We rejected demands that users should have to inform individual data subjects that data were held about them. We considered registration was as far as we could go;

(2) We rejected demands that users should log (a) disclosures, and (b) receipts of data, and we rejected any obligation to tell subjects, individual subjects, of individual receipts of data or disclosures of data;

(3) the bill makes special provision for what we call in the bill, received data, to ensure that users are not required to pay compensation for the holding of inaccurate information received from others as long as that information received from others is marked as such on the data file;

(4) The bill allows a full two years from Royal Assent for users to make the necessary arrangements before the new legal obligations are to be enforced.

We look upon the registrar as far from a dictatorial figure. We see him as assisting data users to understand good data protection practice. We intend

that he should take the initiative himself in spreading the gospel of data protection, giving publicity to the work he's doing and the new rights provided in the bill.

He'll be under, for instance, a statutory duty to encourage groups such as trade associations who represent data users to produce their own codes of good data protection practice in order to assist their members in complying with the principles and so as to reduce, we hope, to the minimum, the number of cases where people actually have to be sanctioned.

We're not so starry-eyed as to imagine that all mistakes and abuses will be prevented, and the registrar's powers to impose sanctions will be needed from time to time. But in structuring our legislative provisions, we have endeavoured to come up with a system that encourages and helps users to put their own houses in order, rather than to concentrate on punishing those who do not.

Just a few words on the response our legislation has had. Data protection is a complex subject and I defy anyone to produce a bill that will suit everyone. But I think we've seen, during passage of the bill, a growing realization of the positive benefits that data protection can bring.

The more far-sighted data users in the private sector are beginning to realize that the necessity of considering their use of computers to hold personal information, the necessity to comply with good data protection practice brings benefits as well as burdens. A number of users are now saying to us that they are surprised how much weeding of files they are finding themselves doing as they prepare for the legislation to come into force.

Much valuable computer practice is being freed for new users. Higher standards of accuracy which the bill will encourage, can only be to the advantage of data users as well as data subjects.

Now finally, Mr. Sterling, I'm not, as you may have gathered, a data protection zealot. In my view, the case for legislation on privacy, on privacy grounds alone, was a very finely balanced one. The number of serious cases of misuse of information brought to our attention was very small, and I don't believe that it's right to introduce legislation without a real need for it being established and without there being a prospect of real benefits flowing from it.

But when the commercial considerations prompted by the convention were added to the plain privacy dimension, and when added also was the importance of calming public fears about the new technology in order to remove barriers to the introduction of computers, then to my mind the case for legislation was proven.

I have no doubt that the situation in Canada is very different. Certainly it would be futile as well as impudent of me to promote our bill as a model to be followed here. Legislation can't be bought off the international peg, and it must be tailor-made to the individual society's needs and must take account of the social, administrative and constitutional background that applies in the case of each country.

Nevertheless, in framing our legislation, we found it helpful to look at how other European countries had sought to cope with the myriad problems that data protection legislation throws up.

I doubt whether our approach in the U.K. will furnish you with many outright answers, but it may give you some help in determing whether to embark on a remotely similar exercise here in Ontario, and I certainly hope that it may have calmed some of the fears of industry and commerce.

Thank you very much for listening to me.

THE PRIVACY ACT: HOW IS IT WORKING TO DATE?

DR. JOHN W. GRACE *
Privacy Commissioner of Canada

One of my favourite observations about the privacy business is a reason why I like my job. It is this: privacy cuts across ideological boundaries. Wherever one is located on the ideological spectrum, there is a shared interest in the values we are here these days to discuss in order to protect and to enhance them.

Some of us came to privacy from different starting places and in different ways. But we end up, whether from the public or the private sector, whether liberal or conservative, asserting that the claims of privacy are essentially claims of respect for human individuality and, ultimately, for human dignity.

A person is diminished by the loss of control over the little pieces of himself or herself tricked out by the supposed needs of society, catalogued, compiled and cross-matched, sometimes for no other reason than that wondrous machines need to be justified.

My twin teen-age daughters recently came home with a record on which Michael Jackson (yes, the Michael Jackson of which there is no other) and someone called Rockwell sing these lines:

"Somebody's watching me
Ain't got no privacy."

It was, they said, my theme song.

Of course, I immediately adopted it. The re-iterated cry from a hero of popular culture that his quality of life is suffering because he "ain't got no privacy", was the ultimate approbation for the need of a privacy protector. Indeed, for one shining moment, this song rose to first position on, as they say, the pop charts. Privacy made the top ten.

What more do any of us need to justify our being here? We may all bask a little in the reflected glory of responding to the plaintive lament, semi-literate though it may be, of Michael Jackson and Rockwell. Privacy, as I say, knows no ideological barriers.

I am delighted to have been asked to tell you something about the federal Privacy Act. I am billed specifically to address the entirely reasonable question: "How is it working to date?". I will not evade my responsibility. But I am going to tell you how it works before I tell you something of how it is working. I want to take the time to explain the Privacy Act, my role and how I perceive that role.

The first thing I have learned since taking over my job about a year ago is that privacy is a hard subject. I learned that before I came to believe that privacy is an important subject and the Privacy Act is a complex piece of legislation. It is full of talk of "banks" which have nothing to do with money, talk of "exemptions" which don't help at all in tax returns, talk of "access" which has nothing to do with roads, and "compliance" with nothing to do with either loose morals or consenting adults.

I am still little better than an instant expert. But my advice based on hard experience is not to assume either a wide or a deep knowledge of

---

* Dr. Grace is a former member of the Canadian Radio, Television and Telecommunications Commission. Prior to that he was with the Ottawa Journal from 1959 serving in many capacities including Vice-President and Editor-in-Chief from June, 1978 to August, 1980. He was appointed as Privacy Commissioner under the Access to Information and Privacy Acts by Parliament, in June 1983.

privacy concepts. The distinguished coterie of experts with us understand the terms of the privacy trade; indeed, many of the terms and definitions are theirs. But I find, even in the public prints, an astonishing and an abiding - if invincible - ignorance of how my piece of privacy legislation works. Hence, this primer.

The Privacy Act is about the protection of personal information held by federal government (not provincial or private) institutions. Personal information starts with names and its definition goes on to include, among other things, addresses, fingerprints, religion, marital status, identifying numbers and opinions.

The Privacy Act grew out of Part IV of the Canadian Human Rights Act. In its own words, the Privacy Act extends "the present laws of Canada that protect the privacy of individuals with respect to personal information about them held by government institutions and that provide individuals with the right of access (there's that word "access") to such information".

Now there are exceptions to the right of access a person has to his or her personal information. There is argument over some of the exceptions, arguments that are inevitable and healthy. Some critics of the Act think that the exceptions go too far in circumscribing the right to privacy. One hand denies what the other hand gave, some say.

Here are the principle exceptions and I leave it to you to decide if they are reasonable or unreasonable.

1. Information received in confidence from a foreign state, a provincial or municipal government;

2. Information which could be injurious to the enforcement of any law of Canada;

3. Information which would disclose information about another individual;

4. Information subject to solicitor-client privilege.

I suggest that these are all defensible exceptions and a good case can be made for each one of them. What I do caution against is the temptation to claim too broad exceptions for the first kind of information, in particular, information conveyed from a provincial to the federal government. Everyone in government wants to be cautious in a new era of privacy Acts. That is understandable. However, nothing will cause a privacy act to lose credibility faster than invoking exceptions to deny information which would have been released without a privacy act. I am seeing a few such occurrences.

The new Canadian Privacy Act also protects an individual's privacy by preventing other persons - again, with certain exceptions - from having access to that individual's personal information. This set of exceptions allows the release of personal information to a third party for such reasons as:

1. To comply with a legal document such as a warrant or subpoena;

2. To an investigative body, such as the RCMP, to enforce a law;

3. To a member of Parliament to assist a constituent when the information relates to the constituent.

Again, there will be argument over some exceptions and the extent of the exceptions. But there can be no serious quarrel with the principle of exceptions. Privacy, like most rights, cannot be absolute. I think it important that privacy advocates be the first to acknowledge this as they enunciate privacy principles. In an open society a dynamic tension will always be in play between the individual's right to protect and to know his or her personal information, and the state's perceived duty to the public interest. We are usually talking about competing goods; not good versus bad.

Particular kinds of personal information which are not available upon application under the Privacy Act are designated as exempt from access -- another term of art. Such information may be contained in information systems which are totally

exempt. Nineteen of a total of some 2200 banks are thus designated. Some personal information in accessible banks may also be exempt from the general right of access. It is these exceptions and exemptions which mean business for the Privacy Commissioner.

The architects of the Canadian legislation had before them the model of an American privacy act where there was no Commissioner. Persons who believed that they had been denied privacy justice had (and still have) no recourse except to apply to the courts for relief. Ged Baldwin, who perhaps more than anyone else is responsible for the existence of a Privacy Act in Canada, has told me that he hoped that the existence of a Privacy Commissioner would save excessive and expensive recourse to courts already overburdened.

Thus, the Privacy Commissioner, with the full powers of a Superior Court Judge, investigates complaints by individuals who think that they have been denied rights concerning their personal files. Because he can be appointed only after a joint resolution of the Commons and Senate, he is independent of government, responsible to Parliament. In order to be effective, it is essential that a Privacy Commissioner enjoys such independence and is not perceived as an agent of the government of the day.

In his role of acting on behalf of individuals, and investigating their complaints, the Privacy Commissioner is a specialized ombudsman. But seeking privacy rights for complainants does not always mean that the Privacy Commissioner will recommend release of personal information. That misconception has arisen recently.

The Privacy Commissioner's duty is to assist individuals in achieving what they are seeking. But the Commissioner cannot manufacture privacy rights. He can only recommend rights to which complainants are entitled. To recommend always in favour of the complainant may give the Commissioner and the public some psychic satisfaction. But the Privacy Commissioner has wider responsibilities under the Privacy Act which cannot be abdicated for the sake of a popular decision. It is naive and simplistic to suggest that the Commissioner recommend in favour of a complainant, whatever the Privacy Act says or whatever the facts of the case. In the long term, such excess would be harmful to the cause of privacy protection.

Once the Privacy Commissioner has all the facts and the balance seems even, he will decide in favour of the individual seeking his personal information. If he is allowed any bias, it is towards the complainant. But to deny the wider provisions of the Privacy Act and to ignore the restrictions which Parliament placed on an absolute right to receive personal information would be to flout the law. Hardly the appropriate role of an ombudsman, no matter how dedicated!

In addition to responding to complainants, the Privacy Act imposes the duty upon the Privacy Commissioner to monitor and report to Parliament upon the manner in which government institutions collect, retain and dispose of personal information. This responsibility, still not generally recognized, broadens the nature of the Commissioner's role beyond that of ombudsman.

He is what I call an auditor-general for privacy, examining files in order to determine whether the personal information they contain is appropriate to the work of a department or agency. The closed or exempt information banks compel themselves particularly to the attention of the Privacy Commissioner. He is the only outsider who can perform an audit of these banks. The possibility of such an audit should have a salutory effect upon the standard of government record-keeping.

Of course, there will always be complaints and the need to investigate them effectively cannot be over-stated. But in the long term, the audit role will be at least as important as complaint-handling. If privacy protection principles are followed, individuals will have no valid reason to complain. Such a state of privacy perfection may be

impossible to attain. But that should be the goal.

The challenge of performing effective compliance auditing is daunting. There will be no army of auditors; nor should there be. The goal will be to make effective use of a small number; my initial complement is five.

A few more facts about the Canadian Privacy Act: for the first time, a complainant may apply to the Federal Court for a review of a refusal of an application made under the Act. In order to go to the court, it is only necessary that a complaint be first investigated by the Privacy Commissioner, not that the Commissioner's finding was favourable to the complainant. The Privacy Commissioner himself is empowered to apply, with the complainant's permission, to the same court for a review of a refusal to accept his recommendations made on behalf of an individual.

The Privacy Commissioner does not have the authority to make an enforceable order. If he finds a complaint is justified, the Commissioner then makes a recommendation to the head of the government institution that the original decision be modified.

If the government institution refuses, the Commissioner has other recourse than asking for a review and an enforceable court order. He may report this denial to Parliament in his annual report, or, if he considers the matter sufficiently urgent and important, he could make a special report to Parliament. The efficacy of the threat of such reports on public service managers should not be underestimated. The Privacy Commissioner is not a toothless tiger far from it.

But his effectiveness rests essentially on moral suasion and on credibility. The independence and integrity of his office, the importance of judicious decisions cannot be over-stated. If the Privacy Commissioner made findings unsupported by the authority of the Privacy Act, he would deserve to be written off as a captive of a populist fancy.

That's the overall view of the main lines of the Privacy Act, with a little homespun philosophy. The question "how is the Act working" will take less time.

The easy way out would be to say its too soon to tell. That would be safe and justifiable. But I think I can say that the Privacy Act is working much better than some of its critics had predicted. And it is certainly not too early for me to report that Canadians are using their Privacy Act. In the first six months after the legislation came into force, almost 10,000 requests for personal information were received by federal institutions.

The statistics are the more impressive because all these applications have been made without benefit of a publicity campaign. You do not hear television commercials or read advertisements telling you of your rights under the Privacy Act. Perhaps you should: I'm not sure about that. Certainly, I have no mandate to conduct such a campaign. This is privacy, not "Participation".

But it is 1984, a year which George Orwell single-handedly has caused to be an international year of data protection. Moreover, privacy applications are free, and the fact of a new Privacy Act gave an initial impetus to applicants. A truer test of public use of the Act will be next year's statistics.

Privacy requests usually obtain results: 80 percent of applications received all or part of the information they sought; only three percent of requests were totally denied.

During this same initial period, 140 complaints were made to the Privacy Commissioner, all of which will receive formal findings.

Three of these cases have gone to the Federal Court for review. The first judgment was handed down a couple of weeks ago by Mr. Justice James Jerome. He upheld the decision, made by a federal department and concurred in by the Privacy Commissioner, to exempt certain personal material from access by a complainant. Three cases in almost a

year: certainly no flood of litigation. I cannot say how many cases the Privacy Commissioner succeeded in keeping out of court.

What I can say, however, is that in a significant number of complaints the intervention of the Privacy Commissioner's office resulted in changes of original decisions in favor of complainants.

Here the role of privacy co-ordinator - those persons named by each government department and agency to handle Privacy Act matters - is crucial. The importance of effective co-ordinators to the proper functioning of the Privacy Act can hardly be over-estimated. I am pleased to be able to say that many co-ordinators are superb professionals. The presence of some of them at this conference is its own tribute to their seriousness and commitment to what might have been perceived in a department as a rather suspect violation.

In addition to complaint handling, the Privacy Commission is becoming a clearing house for queries about privacy. These queries require responses rather than a finding. Responding to such questions and concerns is a function of this office which I think important. It means that the Privacy Commission is being recognized as a resource centre.

You may be interested, though perhaps not surprised, to learn that a large number of questions are about a subject which is not mentioned as such in the Privacy Act:about the use - and abuse - of Social Insurance Numbers. That's another speech!

The Public Service of Canada has lived with privacy legislation for more than five years. The Act means that another regulator is looking over the shoulder of public servant managers. But I can report a remarkably high level of co-operation and support. Privacy no longer needs to be sold.

I have been talking about legislation, the legislation in which I play a part. But privacy protection need not wait for new laws coming into force. I commend initiatives now being taken in the private sector where codes of personal information principles and practices are becoming part of company policy. A time may come when a data protection audit is as commonplace as a financial audit.

The public is not going to tolerate two standards of privacy protection: a relatively high standard for personal information held by the federal government and an indifferent or inadequate standard for provincial governments and the marketplace.

Federal public servants now have access to their own personnel files as a matter of right under the Privacy Act. Employees who may not see their records are going to feel like second-class citizens. They will not be long satisfied with such status. They will achieve those rights, as some have already, under collective bargaining agreements or through the political process.

Of course, many provisions of the Privacy Act go against the political and bureaucratic grain; against an honourable and paternalistic tradition of using personal information in the best interests of government, not necessarily of the individual. These same provisions also go against imbedded instincts and practices of the private sector. The Privacy Act may make the challenge of running an efficient bureaucracy or a business more difficult.

But I should remind you that a broader application of privacy legislation was foreshadowed by the Honourable Francis Fox, the Minister of Communications, in speaking to the Commons during passage of the present Act. He said that the expansion of the number of government institutions covered by the Act "paves the way for the next stage in the development of privacy legislation, extension of the principles respecting the protection of personal information to the federally regulated private sector". There should be no surprises.

Privacy protection, limited though it has been, is nothing new. Confidential-

ity has been enshrined in the medical and legal professions. It is very much in the interest of banks to guard the privacy of their customers. Cable and computer companies also have a vested interest in data protection.

Why, then, the need for legislation and voluntary privacy codes? What is new, is the computer and its wondrous works. The ability to store and communicate vast quantities of data has made a quantitative as well as a qualitative impact on our society because information is power. And that impact has the potential of changing the balance between the individual and the state, between the individual and the private gatherers or storers of information.

Those of us who work as data protectors are doing nothing less than trying to see that the balance is not tipped dangerously against the individual. That is a bold, even a presumptuous, claim. But it is a claim for human freedom and dignity, one that I am proud to make.

PART C

CONFERENCE PANELS

PANEL 1: PRIVATE SECTOR PANEL: "PRIVACY: THE PROBLEMS DEFINED"

CHAIRMAN: Jake Knoppers *

PANELISTS: James L. Kirschbaum

Dr. William R. Ghent

Ross McFarlane, Q.C.

COMMENTATOR: Professor Peter Burns **

---

* Mr. Knoppers, based in Ottawa, has been a specialist in the area of information policy and information technology for a number of years. He is Senior Vice-President of Infoman Inc., a company specializing in information management services.

** Professor Burns graduated in law from Otago University in New Zealand with both LL.B and LL.M in 1963. He was a Barrister and Solicitor with the Supreme Court of New Zealand before coming to Canada. He has been actively involved with the Canadian Bar Association and many other groups as well as working as a consultant. He is the Dean of the Faculty of Law of the University of British Columbia and is widely published in the legal field including works on privacy and the question of the protection of personal information.

NOTE: Bio-data on all Conference participants is included in this publication. The title page for each panel will cover Panel Chairmen and Commentators. Bio-data on Panelists is given on the first page of each panelist's presentation.

PRIVACY ISSUE:
THE PROPERTY & CASUALTY INSURANCE INDUSTRY

JAMES L. KIRSCHBAUM *
Chairman and Chief Executive Officer of
Fireman's Fund Insurance Company of Canada

Four years ago I arrived in Toronto. Believe it or not my wife's primary motivation in agreeing to the move was the fact I could use the transit system as an alternative to a busy freeway. So blissfully I headed for the subway station for my first day in the office. Since I had an empty briefcase I stopped and purchased a newspaper. Settling back to enjoy the leisure and the news, I was amused to read the headline "Insurance Companies Now Want to Know About Your Sex Life".

My amusement turned to shock when I discovered the insurance company was none other than my own, Fireman's Fund of Canada. The story was picked up all across North America and needless to say, the first day on the job turned out to be vastly different than originally planned. Actually, our program was a pretty good one -- psychological testing of impaired drivers. The self-administered tests were designed to separate the person who learned his lesson from the chronic drinking driver. Before the day was out I was in Frank Drea's office -- he was then the appropriate Minister.

Once we cleared the initial emotional issue with reporters, the only unanswered questions had to do with -- the use, the control and the safeguarding of the information gathered.

I was pleased to learn we had carefully considered the privacy issue. Our insureds completed the questionnaires and returned them direct to us in a specially addressed envelope. One person received them and opened and evaluated them one by one. The evaluation rating only was sent to the underwriter who never did see any of the information. All the responses and results were kept in a locked file to which no one else had access.

As part of my orientation and because of this experience I was pleased to learn the company had a very comprehensive written privacy code. This is gone over with all employees on hire and periodically thereafter. It has been reviewed from time to time for adequacy and application and so far has proven to be very effective.

It is a pleasure to be a participant in this conference and to have this opportunity to represent the Insurance Bureau of Canada. The latter is an organization consisting of 95 companies and company groups who write approximately 80% of all the Property & Casualty business in Canada.

In turning back the clock some ten or fifteen years ago, the whole subject of

---

* Mr. Kirschbaum is Chairman and Chief Executive Officer of Fireman's Fund Insurance Company of Canada. He first joined Fireman's Fund in San Francisco in 1949. He currently holds directorships with the Insurance Bureau of Canada, The Centre for Study of Insurance Operations and the Insurance Advisory Organization. He is Director of Fireman's Fund Insurance Company of Canada and American Express Canada, Inc.

this conference was of major concern to many. At that time increased computer usage was coming in to vogue which triggered a rush to gather new and expanded data. Secondly, occurrences at the time, coupled with events of the then recent past, were being interpreted as or associated with perceived improper gathering and use of information. For example, in many parts of the world there were lingering memories of World War II and the adverse impact information, whether right or wrong, could have on individuals or even entire nations. In the U.S., disclosures about FBI and CIA activities and the Watergate incident helped focus attention sharply on the whole subject.

Many very significant changes have occurred in the Property & Casualty Industry since 1970 as respects information. Contrary to initial concerns or even fears, the age of computerization has not led to problems and abuses. In fact, just the opposite has occurred.

With changed environmental factors, acceptance of different social and behavioural conducts and relationships, new underwriting concepts and techniques, the need to have so-called private and personal information about insureds and/or applicants has changed dramatically. Twenty years ago, underwriters ordered and maintained reports on nearly all individual insureds. These were obtained through independent investigative firms who reported the information from file data and interviews of neighbours and business associates of the insured. Reports were generally fairly lengthy and often very subjective and new ones were periodically ordered with cumulative files maintained.

Presently such reports are very objective and consist largely of factors which are readily adaptable to computer application such as motor vehicle convictions. They are still ordered through independent investigative firms who now nearly always interview the insured or applicant directly and rarely will go to others. The reports are used primarily for confirmation or verification purposes and most companies order them on a fairly small percentage of their insureds.

In the Property & Casualty business, underwriters rarely obtain and use medical information. In those limited instances when they do, physician reports are requested directly through the insured. Most such requests involve automobile insureds and the reports are obtained to verify their current physical condition as it would pertain to their ability to safely operate a vehicle.

Both claim and underwriting files, whether electronic or hard copy, are treated on a very confidential need to know access basis. Further, the employment of such data has been cut back significantly hence the frequency of utilization of files has dropped dramatically. Accordingly, files are simply not out being reviewed and worked on to the extent they were in the past thus reducing potential unauthorized exposure.

In addition, the use of new sophisticated computer security systems, for the data stored electronically, ensures the availability on a "need to know" basis within a company.

Underwriting reports are still referred to as credit reports but it is a generic term only. The so called underwriting credit report usually doesn't provide indepth financial or credit information about a policyholder but rather deals only with information pertaining to the ownership and/or use of the vehicle and factors which reflect the driving experience and/or record of the insured.

With respect to claims, outside reports are ordered on a very small percentage of cases. When they are, they deal directly with some element of the adjustment process which requires outside review and/or verification. They could deal with specifics relative to an individual's financial position since that could have a direct bearing on the settlement process. Also, Claims Adjusters will on occasion order surveillance investigations. These are to determine or verify the degree to which somebody

might be disabled or the extent of injury or damage.

A very decided change has taken place relative to the gathering and sharing of medical information as respects claims. The Industry practice is to obtain and/or share only with the written consent of the insured or third party. Frequently this information is done on a physician to physician basis. Such information and results are treated on a particularly confidential basis with only very limited access. Adjusters today will confirm existence of an injury, for example, but will not share medical information with others unless authorized to do so in writing by the injured party.

There are some misconceptions about the amount of information insurance companies have on people and the degree to which that is shared. There simply aren't any large information data bases in existence either overall or within specific companies. Most companies still do not have very sophisticated linkage of data internally and literally nothing in the way of linkage exists on a multi-company basis. About the only information shared, and this is on a very informal and limited basis, is specific experience information or claims history. The industry does share premium and claims information for overall statistical purposes but this is not by individual insured. Also, where evidence points to potential fraud or other potential criminal activity a company may provide information to an industry sponsored crime bureau. Such cases are fortunately very limited. This organization is staffed with professionals who work very closely with law enforcement agencies.

Some people are under the impression insurance companies sell lists of customers to others. We certainly do not and to date I have been unable to come up with a single other company which employs that practice. Also, some people have expressed concerns about what they perceive is the improper use of telephone soliciting. Some agents and brokers do use the telephone extensively for solicitations. The practice however is fairly limited and has been going on for decades.

With respect to personnel files, I again found significant change especially with regard to what information was collected and how such information was maintained. Because of the dramatic changes in this regard, personnel files today are much slimmer than they were previously. Again, very tight security is maintained.

Quite frequently people will call requesting information about our people. We have a very formal and rigid policy about this and simply do not respond unless authorized by the employee involved to do so.

Since we operate basically in a "white collar" environment, our Workers' Compensation exposures are minimal and we simple don't have medical files on our employees.

Companies now make provision throughout for easy correction to any misinformation which may be developed. With a voluntary access program to one's personnel file, we have experienced minimal numbers of requests from people to examine our files on them. My people feel this is in part due to the fact that some don't understand their priviledges while most aren't interested.

Summary and Conclusion:

As I stated earlier, the means to share massive amounts of personal information simply does not exist in our industry. More importantly, we and our fellow insurers collect far less information today than we did a few years ago, gather it in an improved manner, and have formulated policies to safeguard what we do collect.

Insurance companies have operated for centuries in a fiduciary capacity. While concern for the privacy of individuals is a comparatively recent phenomenon, it has been handled by the general insurance companies as another of

the many areas in which they must protect the interests of their customers, and their employees.

It is our belief the industry is thoroughly aware of the issue of privacy - and has responded very aggressively and positively. Even in situations where alleged deficiencies or abuses existed, and these were very minimal, the industry responded quickly and positively to remove any such real or alleged shortcomings. Symposiums of this nature are helpful since they serve as reminders and also may surface areas which could benefit from additional attention, however we do not believe any additional regulations or legislation are necessary.

It has been a pleasure being part of this conference. Thank you for inviting me.

DR. WILLIAM R. GHENT *
Chairman, Council on Health Care
The Canadian Medical Association, Ottawa

I must state at the outset that I am not the official spokesman for the Canadian Medical Association on this subject. I am the Chairman of the Council on Health Care for the Canadian Medical Association and as such, we are in the process of formulating some guidelines on this present topic.

It has been considered by the medical profession in the past, that our Code of Ethics covered this subject adequately for the protection of the individual patient's rights of privacy and confidentiality.

The medical Code of Ethics that has guided us for hundreds of years, was first formalized by Hippocrates, who wrote, "All that may come to my knowledge in the exercise of my profession or outside my profession or in daily commerce with men, which ought not to be spread abroad, I will keep secret and will never reveal". Succinctly reproduced as Article IV in the C.M.A. Code of Ethics, this principle is stated "Protect the patient's secrets".

Legally the principle of patient confidentiality has been documented in Regulation 448, Section 22, of the Health Disciplines Act of Ontario, "giving information concerning the patient's condition, or any professional services performed for a patient to any person other than the patient without the consent of the patient unless required to do so by law"; is considered to be an act of misconduct by the medical profession. I would like to emphasize the last statement as of importance, "unless required to do so by law"; and return to this later.

The consent procedural guidelines are waived by the medical profession in the case of Life Insurance Companies and Proof of Death certificates, necessary to provide the insurer the grounds for payment of death benefits to the family of the insuree. This is understandable and acceptable, both socially and medically. As a conclusion to the "need to know" group, it is a sin e qua non that the patient is the first to know and the immediate family are of next importance in cases where the patient is unable to transmit personal information.

We now enter a grey zone of legal requirements of the "need to know", "would know" variety or "unless required to do so by law". I will state categorically at the outset that governmental agencies are the most blatent and most pernicious purveyors of the erosion of privacy in the health care field.

There are many examples of this slow invasion of privacy by bureaucrats. This first began with the compulsory notification of communicable diseases, without the patient's permission, and with the advertisement of the disease placarded on the front door of the patient so inflicted. I can still remember the "Measles" sign that decorated our front door when I was a kid. This practice has been abandoned by medical advances but not due to public clamour, unfortunately.

The same communicable disease Statutes still apply to the "social diseases" of our society, and the notification on occasion can have tragic results. However, more and more of the medical profession disregard this law as inappropriate, if not stupid, circa 1984.

---

* Dr. Ghent is a practicing surgeon in Kingston, Ontario and is the Chairman of the Council on Health Care of the Canadian Medical Association. Dr. Ghent has served on numerous boards of hospitals and universities and is widely published in the medical field.

Another example of government "would know" by Statute concerns patients whom a doctor considers medically unfit to drive. The doctor is required, under penalty of law, to notify the Motor Vehicles Branch of this patient, with his diagnosis, and without his consent.

The loss of privacy by governmental decree is most worrisome as Ontario Hospital Insurance Plan and its computers obtain, without permission, the diagnosis and treatment afforded each resident of Ontario who seeks medical aid under the plan. This is an OHIP card, the billing mechanism employed by doctors, on behalf of their patients, to receive payment for their services. It contains name, OHIP number, address, date of birth, sex, diagnosis, treatment and date services rendered. This is signed by the doctor. The average patient has no idea of the personal data that has been transmitted to a government agency, and, certainly, the patient has not personally, actively authorized this release of information. This is made legal by the following quote from the Health Insurance Act: Section 33-2:

> Every insured person shall have been deemed to have authorized his physician or practitioner who performed insured services to provide the General Manager with such information respecting insured services performed as the General Manager required for the purposes of the plan.

I suppose the legal jargon, a "Notwithstanding Section 448, Subsection 22 of the Health Disciplines Act" should be added.

It is interesting to follow one of these information packages from a medical office to its ultimate destination in the great white computer in Kingston.

At least five secretarial staff have access to these cards before they reach the computer. Once computerized, the information is stored for sixty days in the computer, and then it is microfilmed for ongoing storage.

I am assured by OHIP that their files and systems are secure except for a court order release. However, the integrity of the storage system must be questioned in view of the recent computer break-ins by educated High School students. This is, of course, the theme of this conference, and as a member of the medical community, I would like to wish you all success. As far as we are concerned, the interest is long overdue.

The public, by and large, are unaware of the governmental health file that is being compiled about them, and I would think this represents the greatest hazard to public privacy that has ever existed in recorded time. We can be assured by the Ministry of Health that all is well and all is secure, but in all honesty, it must be questioned.

The "would knows" of this world are still with us medically, such as the neighbour who contacts the surgeon to find out what was done to his or her "closest friend". Then of course, the ridiculous state of affairs that arise when there are 13 kids and none of them talk to each other or to their parents. The permutations and combinations of queries about who did what to dear Mother and when, are limitless and irrevocably unanswerable except by next of kin.

There could be a more sinister and sophisticated "would know" group on the horizon - a group of experts who, for a price, will steal from personal health files of OHIP for pre-employment information, blackmail, etc.

The Federal Government has never been noted for its sensitivity to privacy or confidentiality - except for its own ends. The latest example of potential invasion of privacy by search and seizure is contained in Bill C9 - our Security Force Act. At least four clauses in this Bill allow for search of any

premises for any information, including medical upon suspicion of security breach.

Of more immediate concern to the medical profession, is the invasion of patient's privacy to be allowed with Bill C123. This Bill is to establish an investigative protocol for aircraft accidents. One clause would provide an investigator, not a medical person, the legal leave to examine a doctor's medical files of any person who may have had contact with a pilot involved in an air crash.

In conclusion, the medical profession has kept faith with the public; the private insurance carriers have kept faith with the public. The offender, by and large, is the bureaucracy of government - provincial and federal. Formally, I would warn each and every resident of Ontario and of Canada that the confidentiality of your health status is in jeopardy.

ROSS MCFARLANE, Q.C. *
General Counsel, General Motors of Canada Limited
(representing the Canadian Manufacturer's Association)

Introduction

Hugh Rowan pointed out in his paper "Privacy and the Law",[1] that one of the difficulties besetting any discussion of privacy is the meaning or definition of the word "privacy" itself. Privacy is an intensely personal or subjective value - what one person would regard as intolerable, another would dismiss as a minor irritant.

A 1979 Harris poll conducted in the U.S. revealed the following major findings, concerning employee privacy issues:

- Twenty-five percent of the public believed employers asked for too much personal information;
- Almost a third of the public believed business did not do enough to keep employee information confidential;
- Seventy percent of employees believed laws should be passed giving employees a right of access to their personnel files;
- Ninety-three percent of employees believed employers should adopt specific policies to safeguard the information in employee personnel and medical files;
- Ninety-one percent of employees believed employers should be required to inform employees of any information indicating that the health of employees is being affected by conditions at work.

Several Canadian provinces have enacted legislation protecting individual privacy and creating a tort of invasion of privacy - without proof of actual damage. Initially hailed as a significant legal development, the passage of these privacy acts has really been a non-development according to Professor Peter Burns of the U.B.C. Law School in his article entitled the "Law and Privacy: the Canadian Experience".[2]

The high cost of litigation and the embarrassment of having the invasion made public has deterred individuals from using the legislation. Therefore the Acts have not provided real protection to privacy interests.

R. Dale Gibson, Professor of Law at the University of Manitoba in his article "Legal Protections of Privacy" suggests that "the main explanation for the limited impact of privacy statutes is probably that there are not many forms of privacy invasion which are not already well protected by existing legal or social sanctions."[3]

I've mentioned some of the privacy concerns of employees. What are some of the privacy problems of business?

1. Access to Employee Medical Records

Surprisingly, a concern for corporations is the inability of management to get access to employee medical records held by its own company physicians. Companies, through their medical departments, acquire a great deal of medical information about an employee during the course of his or her employment.

---

* Mr. McFarlane was in private practice and then a Counsel at IBM for eleven years. He is now the General Counsel for General Motors of Canada Limited. He belongs to numerous associations and is presently serving as Chairman of the subcommittee on Access to Information for the Canadian Manufacturer's Association.

It is common for employees to put forward their medical condition as an important factor in disputes with their employer. Normally in a civil action, the opposite party can obtain copies of relevant hospital and medical records pursuant to the rules of practice of the court. This is done to avoid surprises at trial and minimize wasting the court's time. Ontario courts have gone as far as to say that non-disclosure of relevant medical records to the opposite party would be scandalous.[4]

Similarly, in employee-employer disputes, management would like to receive relevant medical information that has been obtained by the company's physicians, in order to determine whether the employee's claim is legitimate. The current medical-legal climate, however, seems to promote non-disclosure. The result can be trial by ambush for corporations.

How does this happen? Let's assume an employee-employer dispute occurs in a corporation. It can happen in a variety of ways, for example:

1. An employee is fired for refusing to perform his employment duties. The employee says he is sick or injured and can't carry out the work; or

2. An employee claims that he is eligible for certain disability benefits which are dependent on his medical record; or

3. An employee applies for a transfer to a different job in the company which is refused because the company doctor says the employee is unable to do the work.

So the employer approaches its company physician requesting access to the employee's medical files. Surprisingly, the company physician bluntly refuses to disclose the information.

The Physician's refusal is based upon the Ontario Health Disciplines Act; which defines "Professional misconduct" to mean:

> "giving information concerning a patient's condition or any professional services performed for a patient to any person other than the patient with-out the consent of the patient, unless required to do so by law."[5]

Obviously, the employer is placed at a serious disadvantage in resolving this type of conflict, if the employee refuses to permit the doctor to disclose the medical information. Further, if proceedings result, the employer will not see the medical records until the day of the hearing.

The employee's representatives have all of the necessary medical information relating to the employee's claim including reports, and records prepared by the company's doctors. This is manifestly unfair to the employer, who is compelled to wait until the day of the hearing and is therefore unable to adequately prepare its case.

On the other hand, if the employer had been shown the medical information when the complaint first arose, the employer aware of the specific evidence of an employee's serious medical condition would presumably resolve the dispute quickly, sparing both parties the time and expense of a needless hearing.

There is obviously an area of conflict between the duty which a company physician owes to his employer and his statutory duty to persons consulting him in a professional capacity.

The Krever Commission Report into the Confidentiality of Health Information focused on this problem.

It recommended that legislation be enacted "to make it clear that a professional employee's duty of confidentiality transcends his or her duty to obey an employer's instructions, where those instructions require the employee to reveal information held in confidence."[6]

The 1980 Ontario Court decision involving Dr. Morton Shulman reinforces the point that it is a physician's duty not to disclose patient information even if such disclosure would serve a high social purpose.[7]

We can all foresee situations where the need for privacy should yield to a public interest need for disclosure. One such situation arises where the company physician is of the opinion that an employee would jeopardize his own health or safety, or that of his co-workers, if he continued to perform his assigned tasks.

An example is an employee engaged in the assembly of automobiles, who is subject to dizzy spells. Section 15 of the Ontario Occupational Health and Safety Act places a statutory duty on employers to "take every precaution reasonable in the circumstances for the protection of a worker".

Another example arises where a company doctor becomes aware that the blood lead levels of certain employees exceed permissible levels, suggesting that these empolyees may be exposed to high concentrations of lead. The doctor is entitled to indicate to plant management that there are excessive lead levels in the plant, but is precluded from disclosing which particular employees are affected. Management is therefore unable to take effective action to remedy a potential hazardous situation in the plant.

If employers are to properly discharge their obligations under the Occupational Health & Safety Act to protect workers in the workplace, they must have specific information concerning health or safety risks, including the medical information about the employees involved.

It is clear that amending the Health Disciplines Act to permit some disclosure of medical information is necessary and desirable in these cases.

2. Surveillance

Should companies faced with the inability to obtain medical evidence prior to a hearing, engage in employee surveillance to produce the necessary information? This is particularly so in workmen's compensation cases where the employer knows, or strongly suspects, the employee is a malingerer but cannot otherwise produce the evidence.

The introduction of photographs or video tapes of the employee's activities into evidence may prevent an unqualified claimant from receiving benefits. The admissibility of such evidence is a matter for the presiding judge or tribunal.

Covert surveillance activities obviously impacts upon an employee's privacy. However provided there is no trespass or intimidation involved, such activities do not appear to be prohibited by the criminal law.

As mentioned, several Canadian Provinces have passed privacy legislation creating a tort for the unreasonable violation of a person's privacy. The Saskatchewan and Newfoundland Acts specifically state that auditory or visual surveillance of a person by any means whether or not accompanied by trespass, is prima facie a violation of privacy.

While no one would disagree with the intent of this legislation to protect people from unreasonable violations of their privacy, it can tie the hands of a company who has an employee who is abusing the system and unfairly collecting workmen's compensation benefits.

3. Personnel Files - Collection, Storage and Distribution of Employee Information

Employers collect personally identifiable employee information for a variety of business reasons, such as the proper administration of labour agreements, benefit programs and other business functions or to comply with various federal and provincial laws and regulations. Personally identifiable information includes any information about an employee that can be isolated, such as a name, employee serial number or social insurance number.

There is no question that there has been increased emphasis within corporations

on the fair treatment of employee's records, their confidentiality, accuracy and relevance.

We have found fair information practices and concern for protecting personal employee information to be consistent with good business practices.

In my experience major corporations have procedures, or "Codes of Conduct" which would include most of the following guidelines, for the protection of employees information:

1. Collection and Use of Data

Only such information as is relevant and necessary to the employment relationship should be collected. No records should be gathered or maintained concerning an employee's political activities, memberships, publications or communications of non-employment activities without the written authorization of the employee.

Access to personal employee information should be limited to those persons in the company having a legitimate need for such information in the performance of their job responsibilities. Employees using such information should be instructed as to the importance of maintaining the confidentiality of personal employee information.

All notes, memoranda and letters generated by management and contained in personnel files should be written in a straight forward, objective manner.

2. Disclosure of Information Outside the Company

Personal employee information should not be disclosed outside the company without the employee's written consent, unless required to be disclosed by law or by court order.

The need to regulate disclosure to third parties is becoming more apparent as corporations are increasingly seen to be information sources for parties engaged in, or contemplating litigation. Inquiries include the following;

(a) summary of an employee's work record;

(b) previous periods of absence;

(c) availability of overtime hours;

(d) physical requirements for a specified job;

(e) location of an individual;

(f) personal medical information;

(g) rates of pay and expected increases in pay.

This information should not be disclosed without the consent of the employee concerned.

In a typical situation, information concerning an employee's income is requested by his or her spouse in family court support proceedings. Following company policy, the request is denied and the spouse then proceeds to subpoena the records. The result can be that companies may find their personnel administrators spending almost as much time in court as at the office. Where medical information is requested, the personnel administrator will not have the medical record, with the result that a company can end up with two employees in court, the personnel administrator and the company doctor.

Legislation allowing employers reasonable compensation for their time and expense associated with these information requests would reduce these costs and help eliminate unnecessary requests.

(3) Employee Access to Personnel Files

There is increasing pressure on companies to give employees access to their personnel files. This is seen to be a corollary right to the right of privacy in the files. The federal Privacy Act includes provisions for access to personal information held by a federal government institution about individuals. Recently, a Private Members Bill was introduced in the Ontario legislature amending the Employment Standards Act to give employees in Ontario the right of access to employer's personnel records relating to the employee.[8]

I believe, most businessmen support the principle that employees should have access to their personnel records. It is my experience that employees rarely exercise this right, since most companies now disclose to their employees the employee's performance evaluation rating, during the appraisal process.

4. Privacy of Confidential Technical Information of Suppliers

The transfer of technical information between an owner and a user of the information is common in the high-tech, specialized business environment of the 1980's. Large, diversified multi-national corporations rely on technology developed by outside firms specializing in intellectual property. This property may take the form of computer software, blue prints and drawings, video tapes, audio cassettes, and so on. A privacy concern arises out of the supplier's desire to protect from public disclosure what may be his only major asset - the technical information.

In order to protect its interests in the property, the supplier of the information looks to patent, trade mark, copyright and industrial design laws. Most view such laws as ineffective or inadequate in protecting its valuable information.

Accordingly, suppliers are increasingly seeking to obtain contractual protection for their confidential information through non-disclosure agreements. These agreements permit the supplier to impose upon the recipient far reaching obligations. Recipient companies should be cautious when signing non-disclosure agreements.

The agreements should be for a limited period of time, should only cover written communications and should define the standard of care to be provided by the recipient company. For example the recipient company could agree to give the information the same protection as it does to its own confidential information.

A new twist to the protection of supplier trade secrets and confidential information involves the developing Canadian Workplace Hazardous Materials Information System. Industry, labour and government have worked to develop a system which would permit suppliers of hazardous materials to disclose information about these products to the users, while still protecting the supplier's trade secrets in this information. The information is required by the users to educate their employees on the safe use of hazardous materials in the workplace.

Implementation of this system will balance the conflicting needs of providing the information so that the user can educate his employees, against the supplier's vital interest in protecting its trade secrets.

5. Confidentiality of Business Information

Just as individuals are concerned about the confidentiality of their personal records, companies take great care to protect their confidential business information from disclosure to their competitors and to the public.

As many of you are aware, on July 1, 1983 the Federal Access to Information Act came into force. The laudable objectives of promoting open and accountable government have come under close scrutiny by the private sector whose confidential records, in the hands of government agencies, become subject to public disclosure.

Several provincial governments have passed, or, like Ontario, are considering the passage of similar legislation governing public access to provincial government records.

The past ten months' experience under the AIA indicates that companies have or should become more cautious in their dealings with the federal government out of fear that confidential information will be subject to public disclosure. Relations with government which were once less formal have become formalized; both parties require information requests be put in writing; replies are scrutinized and documents painstakingly stamped "confidential". The exchange of

information between business and government now follows rigid guidelines. The recent Federal Court of Canada Maislin Transport decision suggests that the private sector's concerns are not ill-founded. It is difficult to fully appreciate the significance of this case, because we don't know what the specific financial information Maislin argued was confidential and therefore should not be disclosed.

However it is clear from the decision that "it is not enough for Maislin to treat the information confidentially, but it must in fact be confidential by some objective standard."

The objective standard the court appears to be applying is the U.S. National Parks vs Morten test which held that in order for the information not to be disclosed it must "cause substantial harm to the competitive position of the person from whom the information was obtained."

A U.S. critic stated that the substantial competitive injury test places an almost impossible burden of proof on the submitter. Also gathering the evidence required to keep documents from exposure is so costly only the largest corporations make the effort.[9]

It is hoped that if Ontario introduces freedom of information legislation that it does not impose standards of disclosure that are so onerous as to dissuade companies from freely communicating with their government, out of fear of disclosure of their sensitive information.

Conclusion

The presence of sophisticated electronic equipment used in business today permits information to be collected, collated and distributed quickly and to various recipients. Such capabilities are required to be competitive in today's global economy. What is needed is a balancing of the interests of all parties involved - a delicate balance which will protect the rights of all parties, yet permit the use of society's most valuable resource - information. That is the challenge for government and business today.

FOOTNOTES

1. Hugh Rowan, Q.C., "Privacy and the Law", Law Society of Upper Canada Special Lectures, 1973, pp. 259-307.

2. Peter Burns, "The Law and Privacy: The Canadian Experience", (1976), 54 Canadian Bar Review 1.

3. R. Dale Gibson, "Legal Protections of Privacy", The Practice of Freedom, Canadian Essays on Human Rights and Fundamental Freedoms, 1979.

4. Coderque v Mutual of Omaha Insurance Co., [1970] 1 O.R. 473 (Ontario Supreme Court).

5. Health Disciplines Regulations, R.R.O. 1980, Reg. 448, Section 27(22).

6. Report of the Commission of Inquiry into the Confidentiality of Health Information, Volume III, pp. 167-168.

7. Re Shulman and College of Physicians & Surgeons of Ontario (1980), 29 OR (2d) 40 (Ontario Division Court).

8. Bill 20 - An Act to amend the Employment Standards Act (Reid, Rainy River).

9. Jack I. Pulley, Senior Environment Attorney Dow Corning Corporation, "The Freedom of Information Act - A Government Subsidy of Industrial Espionage". p.11

PANEL 2: PUBLIC SECTOR PANEL: "ACCESS TO INFORMATION: HOW DOES THIS RELATE TO PRIVACY"

CHAIRMAN: Professor Don Rowat *

PANELISTS: John D. McCamus

Professor T. Murray Rankin

Professor David Flaherty

COMMENTATOR: Ken Rubin **

---

* Professor Rowat is in the Political Science Department at Carleton University. He is an internationally known expert on both freedom of information laws and on the role and function of the Ombudsman in different jurisdictions. He is the author and editor of many books on these subjects, including Administrative Secrecy in Developed Countries (Macmillan, London, 1979).

** Mr. Rubin has been involved as a consumer advocate and public interest researcher for over a decade and a half on the local and national scene. He has done extensive research and writing on freedom of information and privacy in Canada. His works include: How Private is Private?, Prying Eyes, The Public's Right to Information Access in the Federal Government and Opening the Door a Crack. Mr. Rubin has been active in food policy issues, in civil libertarian issues, in local community concerns and as an advocate of citizen participation.

THE DELICATE BALANCE: RECONCILING PRIVACY PROTECTION WITH THE FREEDOM OF INFORMATION PRINCIPLE

JOHN D. MCCAMUS *
Dean, Osgoode Hall Law School
of York University

A. Introduction

The freedom of information principle holds that, generally speaking, every citizen should have the right to obtain access to government records. The underlying rationales most frequently offered in support of the principle are, first, that the right of access will heighten the accountability of government and its agencies to the electorate; second, that it will enable interested citizens to contribute more effectively to debate on important questions of public policy; and third, that it will conduce to fairness in administrative decision-making processes affecting individuals.[1]

The protection of privacy principle, on the other hand, holds in part at least that individuals should, generally speaking, have some control over the use made by others, especially government agencies, of information concerning themselves. Thus, one of the cardinal principles of privacy protection is that personal information acquired for one purpose should not be used for another purpose without the consent of the individual to whom the information pertains. Absolute adherence to this principle is thought to be unworkable in practical terms and the principle is therefore typically hedged in by various exceptions in privacy protection legislation. Nonetheless, the principle represents the statement of an ideal from which the exceptions are taken. The philosophy underlying the privacy protection concern links personal autonomy to the control of data concerning oneself and suggests that the modern acceleration of personal data collection, especially by government agencies, carries with it a potential threat to a valued and fundamental aspect of our traditional freedoms.[2]

When one focusses attention on government records containing personal information concerning identifiable individuals, it is manifest that these two philosophies and legislation based upon them are capable of generating conflict. At the risk of belabouring the obvious, a few illustrations of the problem may be listed:

1. A journalist seeks access to government records that will reveal the salaries of the chief executive officers of all Crown corporations.

2. A researcher doing a study of military justice seeks access to records of decisions in disciplinary matters.

3. A journalist who believes that a particular agency has been lax in dealing with a particular problem, seeks access to records which reveal the actions taken by responsible officials.

4. A convicted offender, released from prison under supervision, commits an offence of violence. A journalist seeks access to letters written in support of the prisoner's release.

---

* Dean McCamus has been serving as the Dean of Osgoode Hall Law School, York University since July 1, 1982. He was the Director of Research of the Ontario Commission of Freedom of Information and Individual Privacy. He has written extensively and is often in demand as a conference speaker on the subject of access to information and privacy. He is editor of "Freedom of Information, Canadian Perspectives" (Butterworths, 1981).

5. A journalist seeks access to government records which he believes will reveal that a public servant has engaged in improper financial dealings with public funds.

One could easily multiply examples of this kind. In each case, the individual seeking access wishes to scrutinise some aspect of the conduct of public business. In some cases, this will involve disclosure of information pertaining to public officials. In others, it will involve disclosure of information concerning ordinary citizens. In each instance, the subject of the information can plausibly raise a privacy protection concern. One man's freedom of information is another man's invasion of privacy.

The conflicts thrown up by these tensions between the freedom of information and privacy protection principles give rise to essentially three policy problems for those who are engaged in designing legislated freedom of information and privacy protection schemes. First, there arises the problem of institutional design. In what institutional forum should conflicts of this kind be resolved? In the courts? In the legislature? In the bureaucracy? Second, wherever these problems are to be addressed, what guidance can be given to those saddled with the resolution of such conflicts? This is the question of substantive policy. How, if at all, can these two conflicting values be reconciled? In this paper, I will attempt to address these two questions and will do so against the background of a comparative analysis of Canadian and American freedom of information and privacy protection statutes and the proposals of the Ontario Commission on Freedom of Information and Individual Privacy, set forth in the Commission's 1980 Report, Public Government for Private People.

A third range of problems, essentially technical in nature, will not be addressed here. These problems arise from the potential for conflict between the general rights of access conferred by freedom of information laws and the more particular rights of access conferred by privacy protection laws which enable individuals to obtain access to information concerning themselves. It is no easy task to design access rights within these two different contexts which will co-exist harmoniously, and this has proven to be a continuing problem in the American federal experience.[3]

Suffice it to say that in the Canadian context, these problems appear to have been for the most part resolved in the drafting of the federal Access to Information Act and the Privacy Act, as enacted in June of 1982.[4]

B. The Institutional Design Problem: The Locus of Conflict Resolution

Since conflict between the competing values of access to information and personal privacy appears inevitable, what is the ideal institutional location for the power to provide an authoritative resolution of these conflicts? The answer provided by the American federal legislation is, as with so many other points of difficulty in the American freedom of information and privacy protection schemes, that the ultimate recourse is to be taken to the courts through judicial review of agency decisions to deny access.[5] The U.S. Freedom of Information Act requires that federal government agencies make their records available to "any person" unless the records fall within one of nine exceptions to this general rule. The exception of relevance to the present discussion is that agencies may refuse to disclose "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy"[6]. An individual who is denied access to a government record on the basis of the agency's conclusion that disclosure would be an unwarranted invasion of privacy, may challenge the agency's decision in the federal courts. The court will, in turn, reach its own conclusion as to whether or not the record is exempt from disclosure and, if satisfied that the public interest in access outweighs the individual data subject's interest in privacy, will order disclosure of the doctrine in question.

The U.S. Privacy Act[7] is drafted so as to function consistently with the access

scheme. Thus, although the Act generally prohibits disclosure of personal data without the consent of the data subject, there are some exceptions to this general rule and one of them permits disclosure under the Freedom of Information Act. Thus, the Freedom of Information Act confers a right of access upon the requestor, the content of which is subject of judicial determination, and the Privacy Act confers a right of non-disclosure on the data subject, the content of which can again be tested in the courts. To be sure, for the litigation-averse public servant, a premium is placed on sound judgment. When confronted with a request for access to a record containing personal information, the agency confronts the twin possibilities that if it denies access it may be sued under the Freedom of Information Act whereas if it grants access, it may be sued under the Privacy Act. Nonetheless, the American scheme does provide an independent source of authoritative advice on the resolution of the tension between access and privacy values. It is not at all surprising that a sophisticated jurisprudence on this question is emerging in the American case law.[8]

Under the Canadian federal legislation, by way of contrast, reconciliation of the access and privacy values is left essentially to the discretion of public officials. Thus, although the Access to Information Act[9] confers a broad right of access to government records - a right which is for the most part subject to enforcement by the courts[10] - it exempts from this right access records containing "personal information", this latter concept being very broadly defined indeed in the statute.[11] This definition is itself subject to certain limited exceptions with the result that a very narrowly-conceived right of access to records containing personal information is contained in the Access to Information Act. As a general rule, however, access to such records is prohibited by the statute,[12] although this prohibition is, in turn, made subject to whatever disclosures are permitted under Section 8 of the Privacy Act. The latter provision is the section of the Privacy Act which purports to control disclosure of personal information. Although it begins by stipulating that personal information shall not be disclosed without the consent of the individual data subject, it goes on to confer a series of discretionary powers on agencies to disclose information to a variety of individuals for a variety of purposes and concludes, in sub-section (m), that an agency has a discretion to disclose:

> ...for any purpose where, in the opinion of the head of the institution,
>
> (i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or
>
> (ii) disclosure would clearly benefit the individual to whom the information relates

The language of sub-paragraph (i) evinces a strong bias in favour of privacy protection, in contrast to the American provision which evinces strong support for the access principle, but this is a point to which we shall return in the next section of this paper. The important point for present purposes is that, as far as personal information is concerned, essentially no right of access is conferred upon individuals seeking access and no right to control disclosure is conferred upon those who wish to prevent it. In sharp contrast to the American scheme, then, the Canadian statute confides this entire question to the discretion of agency officials.

In short, the Canadian scheme addresses the problem of resolving the conflict between access and privacy by simply surpressing it into the level of administrative discretion and withholding rights of access and rights to prevent improper disclosure.

In adopting this approach, the Canadian scheme has, in my view, both substantially undermined the access rights conferred by the Access to Information Act and significantly depreciated the degree to privacy protection afforded by the Privacy Act. As far as the access right

is concerned, it should be emphasised that a very substantial percentage of government records must contain information pertaining to identifiable individuals which would bring them within the sweep of the far-reaching definition of personal information contained in these statutes. To confer so broad a discretion on the federal bureaucracy to withhold or disclose such information is to simply ignore the basic premise of freedom of information legislation, i.e. the conferral of a right of access on the public at large. Public officials are placed in a position of conflict of interest when asked to disclose information which might facilitate effective public scrutiny of their performance. The enactment of a freedom of information statute represents an acknowledgement of this plain fact and the adoption of a remedy which places the decision to disclose the document effectively beyond the powers of the officials concerned. If it is the point of the federal Canadian scheme to sacrifice freedom of information in order to effect a high level of privacy protection, then it must be said that the federal bureaucracy is also not the most suitable instrument for the achievement of this objective. Again, public officials when charged with the responsibility for weighing privacy values in the context of an access request, are placed in a conflict of interest position. It may well be in the interests of a particular department to disclose information and demonstrate that is has conducted public affairs in a perfectly sound and responsible fashion, notwithstanding the substantial invasion of the privacy of identifiable individuals which may result from disclosure.

A leading American decision under the Freedom of Information Act illustrates the problem. In Sonderegger v. United States Department of the Interior,[13] certain journalists sought access to claims files arising in the context of special federal assistance programmes for the victims of a flood which had devastated a town in Idaho. The journalists obviously wished to detect malfeasance in the handling of such claims and the federal agency involved was quite willing to permit full disclosure. The flood victims, on the other hand, felt that disclosure would substantially invade their privacy, inasmuch as each claim represented essentially the net worth of the individual in question. As well, they felt that disclosure would prove to be very stressful for a community which was already enduring considerable stress in attempting to re-establish itself after this disaster. Expert evidence was provided by a psychologist who was working with the local committee, confirming this prognostication. The federal court decided that the public interest in disclosure was significantly outweighed and, thus, overruled the decision of the agency to permit disclosure. One can understand that public officials are anxious to dispel unfair allegations of wrongdoing. My point simply is that there will be situations in which the question of disclosure cannot be approached in a completely disinterested fashion.

A substantial problem with the Canadian scheme, then, is that it establishes a far-reaching domain of discretionary power which, at one and the same time, creates the risk that access to records will be denied in order to preclude appropriate scrutiny of public affairs on the pretext that disclosure will unfairly invade the privacy of data subjects and, on the other hand, the risk that public officials concerned to clear their good names will be tempted to do so, notwithstanding the fact that disclosure will effect a substantial invasion of the personal privacy of individuals.

A further problem with the Canadian scheme is that it conduces to a wilderness of inconsistent decision-making from one department and governmental unit to the next. One finds little or no guidance in the statute itself as to how the discretion to disclose should be exercised. More surprisingly, perhaps, neither does one find assistance in the Treasury Board's Interim Policy Guide which sets forth extensive guidance for public officials on the proper interpretation and implementation of other aspects of the Access to Information Act and the Privacy Act.

A more sympathetic observer of the Canadian scheme might argue that the problem is, after all, an intractable one and suggest that the legislation in its current form will at least provide a splendid opportunity for the Information Commissioner and the Privacy Commissioner to investigate matters of this kind and assist the bureaucracy in developing helpful guidelines for resolving conflicts of this kind. It is difficult to discern, however, that either Commissioner will have a substantial role in dealing with this issue. As far as the Information Commissioner is concerned, if the information in question clearly falls within the definition of personal information, and surely this will often be so, there does not appear to be much for her to say, other than that the record in question is, indeed, exempt from the access scheme. As far as the Privacy Commissioner is concerned, provided that the public official in question has, in good faith, weighed the public interest in disclosure against the privacy value, it is again difficult to see that much remains to be said by the Commissioner. It may well be however, that given the importance of this question and the absence of any other source of guidance, either or both Commissioners will see fit to comment either on the inadequacies of the current legislative scheme or on the deficient exercise of the discretion which is unquestionable conferred upon public officials by it.

Two further explanations may be offered for the Canadian reluctance to extend judicial review into the area of personal records. First, it may be felt that this is an attempt to avoid burdening data subjects with either the cost or the inconvenience of participation in judicial review. Second, it may be thought that so important a question as this ought not to be simply remitted to the courts.

With respect to the first point, a preferable solution would have been to endow the Privacy Commissioner with the power to bear the cost of litigation of this kind on behalf of the data subject. One of the great innovations of the Access to Information and Privacy Acts was to confer a power of this kind on both the Information Commissioner and the Privacy Commissioner in the context of access requests. Where either Commissioner believes that the information should be made available over the objection of the governmental institution in question, the Commissioner is entitled to carry litigation brought on behalf of the requester and thus provide an authoritative resolution of the dispute which is cost free to the requester.[14] The Privacy Commissioner could have been similarly empowered to provide cost-free litigious protection to the data subject.

With respect to the appropriateness of the courts as the instrumentality for resolving these conflicts, it would appear that the only other alternative to the bureaucracy itself would be the legislature. Indeed, many statutes which establish administrative mechanisms requiring the collection of personal data do explicitly provide for the protection of the data and, while the notion of resort to the legislature has an obvious democratic appeal in this context, two reservations about the capacity of the legislature to deal effectively with these issues must be registered. First, a legislature dominated by a majority party is easily seen to be subject to a version of the same conflict of interest that plagues the executive branch. The Access to Information Act notwithstanding, a Canadian government is not likely to vigorously pursue a policy of drafting legislation so as to ensure effective scrutiny of its own conduct of public affairs. Secondly, it should be noted that many legislative provisions of this kind are currently to be found in the statute book and, consistently with the hypothesis just stated, they typically provide that there is to be no access whatsoever to the data in question. The concern that such provisions may conduce to too much secrecy is manifested in Section 24 of the Access to Information Act, which requires that all such provisions be reviewed by a Parliamentary Committee within three years of the enactment of the Access to Information Act. Accepting, as I do, that provisions of this kind relating to personal data were often enacted purely for privacy protection purposes, they

are typically drafted without any apparent sensitivity to the desirability of permitting some forms of access to even reasonably sensitive data. Thus, as Professor David Flaherty demonstrated in a paper prepared for the Ontario Commission, much useful medical research has been thwarted by the existence of provisions of this kind.[15] Leaving these reservations aside, however, it nonetheless is true that one possible response to the concern that the courts should not be given too much discretion in matters of this kind would be to specifically enact access and disclosure schemes to deal with specific information contexts.

As a more general matter, however, there are a number of difficulties inherent in the current Canadian model of administrative discretion and in a general referral to the legislature. This, together will what appears to be reasonably positive American experience suggests that judicial review is the most attractive of the alternatives. Whether the reconciliation of privacy and access principles is to be located in the legislature or the courts or the bureaucracy, or perhaps all three, the difficult question that remains, and to which we now turn, is how one should approach the task of effecting that reconciliation in analytical terms.

C. The Substantive Problem: Achieving an Appropriate Balance

Again, the American and Canadian models provide interesting points of contrast. As has been indicated, the American statute provides a right of access unless disclosure of personal data would constitute a "clearly unwarranted invasion of privacy". The Canadian statute, on the other hand, provides for essentially no right of access, but for the right to obtain documents containing information in three categories:

1) Certain basic information concerning the contracts of employment of public servants and their opinions or views given in the course of employment;

2) Similar information concerning individuals performing services for a government institution under contract; and

3) Information "relating to any discretionary benefit of a financial nature, including the granting of a licence or permit".[16]

Presumably, the draftsmen of the Canadian statute thought that a more precise provision of this kind had some advantages over the vague standard of the American "clearly unwarranted invasion of privacy" test. Nonetheless, the difficulties created by a refusal to embrace a balancing test of some kind are manifest in this provision. As an access right, the Canadian provision leaves much to be desired. The illustrations with which I began this paper were carefully chosen with this point in mind. They are all situations in which, in my view, a strong claim for access can be made and they are all situations in which access would be granted under the American scheme, notwithstanding the fact that all involve disclosure of personal information.[17] They are also all situations in which no access would be given as of right under the Canadian statute.

From the privacy protection point of view, the Canadian provision is also flawed. Although one understands the obvious rationale for requiring disclosure of information relating to discretionary benefits such as licences, it should be noted that most welfare schemes, perhaps all such schemes, contain modest discretionary features. Thus, whether we speak of unemployment insurance benefits or widows' benefits under veteran's assistance legislation, or the various forms of assistance rendered to those suffering from mental or physical disabilities, some financial benefits typically remain within a discretionary category. There appears to be no merit whatsoever in conferring, as the Canadian statute does, a right of access to personal data pertaining to discretionary benefits of this particular kind.

A strong case can be made, then, for the desirability of a balancing test of some kind. Indeed, this is accepted in the

Canadian statute to the extent that apart from the limited right of access to personal data conferred in the Access to Information Act, all other disclosures are to be made - though purely as a matter of administrative discretion - on the basis of a balancing test. The question that remains to be considered is how this balancing test should ideally be designed. Before offering some suggestions to this end, two preliminary points can usefully be addressed.

First it should be noted that to some extent the conflict between freedom of information and privacy protection can be resolved be deleting the names of identifiable individuals before releasing the requested documents. Anonymous data of this kind will often meet the needs of the requester and retard, if not completely eliminate, the risk of privacy invasion. As the leading U.S. case of U.S. Department of the Air Force v. Rose[18] indicates, however, even where some risk of identification or privacy invasion remains, deletion of names may make the task of balancing the public interest in access against the risk of privacy invasion an easier one. In Rose, legal researchers engaged in a study of military discipline sought access to records relating to Air Force disciplinary proceedings. They conceded that access to records with names deleted would be sufficient for their purpose but it was objected by the defendant that even with names deleted, it would be possible in many instances for individuals who were familiar with the incidents in question to identify the person disciplined. The federal court held that although this risk was present, it was outweighed in the present case by the public interest in the ability of outsiders to scrutinise this area of government activity.

In any case where the deletion of names or other identifying detail has the effect of preventing the identification of individuals, the requester should be able to rely upon the principle of severability, i.e. the principle embraced by both the American and Canadian access statutes that the government must disclose any reasonably severable portion of a requested document that is not covered by one of the exemptions.[19] One of the lessons of the Rose case, however, is that even where the elimination of identifiability cannot be achieved in this way, one may nontheless reduce the risk of privacy invasion to the point where it is outweighed by the public interest in access.

A second point which has surfaced in the American case law applying the "clearly unwarranted invasion of privacy" test is whether the specific use of the personal data proposed by the requester is to be relied upon as the basis for testing the public interest in disclosure. Thus, where the requester has some highly beneficial medical or other research in mind, is it the potential benefit of such research that should be weighed against the invasion of privacy or, inasmuch as disclosure is likely to mean that the personal data can have a wider circulation in the public domain, should the particular use of the requester be ignored? In the U.S. experience and literature, discussion of this issue has been provoked by the decision in Getmen v. NLRB,[20] a case in which certain law professors specializing in labour relations were allowed access to lists of employees eligible to vote in union representation elections in order to carry out research on certain policies of the U.S. National Labour Relations Board relating to the certification process. The court in Getman awarded access to the requesters specifically for the purpose of this project, and on the faith of an undertaking by them that they would not disclose the names of the individuals to anyone else. It is not at all evident that the disclosure of these names to the public at large would be sustained. Indeed, given the apparent absence of any public benefit from such disclosure, this would likely be characterized as an unwarranted invasion of personal privacy - hence the Getman court's concern that the requesters make no further disclosure of the employee lists. In Getman, then, the Court was prepared to grant limited access to the particular requester, even though access to the public at large would be inappropriate.

The debate stimulated by Getman has been rather intense.[21] Some have objected to the decision on the grounds that inasmuch as the Freedom of Information Act provides access to "any person", the particular requester's "need to know" ought to be considered irrelevant. Others have had a policy justification for this reading of the statute which, to my mind at least, is compelling. If one does embrace a "need to know" concept in some of this case law, it is likely to spread its influence throughout the case law dealing with the conflict between freedom of information and privacy protection and very substantially undermine the value of the access right. Moreover, it seems impractical to contemplate a general practice of trying to restrain further disclosures of information released to requesters under the Freedom of Information Act. A far better solution, it seems to me, and one that was in fact proposed in the report of the Ontario Commission, was to treat the problem of access for research purposes as a separate problem and to devise a mechanism for providing access to personal data for the research community.[22]

Turning then to the central question, how is one to strike a balance between freedom of information and privacy protection, the question essentially is whether one can do any more by way of providing guidance to decision-makers than to offer the general instruction provided, albeit in significantly different terms, by both the American and Canadian statutes that the decision-maker should carefully weigh the public interest in disclosure against the personal interest in privacy protection. My own view is that one can substantially improve on this approach by attempting to articulate a variety of more explicit factors that should be taken into account by someone undertaking the task of reconciling these two interests. The following propositions derive, in the main, from discussion set forth in the Ontario Report[23] to the same general effect and from a reading of the American case law applying the "clearly unwarranted invasion of privacy" test.

I would suggest that the following factors should be considered pertinent in attempting to balance these conflicting interests:

(a) Is access to the information necessary to enable an individual to accomplish any of the objectives underlying freedom of information legislation, i.e. effective scrutiny of the activity of government institutions, effective participation in discussion concerning public affairs and increased fairness in administrative decision-making affecting individuals.

As I have already indicated, it may be asking too much of human nature to allow public officials themselves to determine whether a particular request is well suited to accomplish these objectives. The issues raised by these criteria for access are not particularly subtle, however, and could be answered with some confidence by third parties in most instances.

(b) Is access to the information in question likely to make a positive contribution to the promotion of public health or safety?

In addition to the generally accepted political rationales articulated in point (a), the granting of access to information with health and safety objectives in view appears to be accepted as a desirable spinoff of freedom of information legislation. Requests put forward to these reasons offer a particularly compelling interest in access.

(c) Will access to the information in question promote an informed choice in the purchase of goods and services?

Again, this appears to be a desirable incidental spinoff of freedom of information schemes. It is of no little interest that items (b) and (c) both find some philosophical support in Section 20 of the Canadian Access to Information Act which explicitly provides for access to the results of product and

environmental testing and, more generally, confers upon government institutions a discretion to disclose commercial information if the public interest in public health, public safety or protection of the environment outweighs the harm that might result to the commercial party to whom the information pertains.

(d) Will the granting of access have the effect of benefitting the individual who is the subject of the information disclosed?

There may well be situations where the individual seeking access has only in mind the conferral of some benefit on the data subject and the case for disclosure in such circumstances is obviously compelling. This consideration is explicitly set forth in Section 8(m) of the Privacy Act as a basis for exercising the discretion to disclose.

(e) Is the information of a kind which is normally disclosed in other contexts?

The fourth illustration set forth at the beginning of this paper asked whether letters written in support of the release of a prisoner should be available to the public. These were the facts of a decision under the American Act, Philadelphia Newspapers, Inc. v. U.S. Department of Justice,[24] in which the court reasoned that inasmuch as such individuals are acting, in a sense, as character witnesses for the convicted person, something they would normally be required to do in a public hearing, their letters should be made available. Here, as elsewhere in legal analysis, fruitful analogy is an important source of guidance.

A number of factors may be taken to weigh in the balance against disclosure:

(f) Will access to the information frustrate the objectives of the statutory scheme under which the information was originally collected?

There may well be situations, for example, where conciliation procedures are mandated by a statute, where a disclosure of records will render the governmental institution in question effectively unable to carry out its assigned statutory task. Surely this would weigh heavily against disclosure.

(g) Is the personal information of an especially sensitive kind?

It is possible to identify types of information such as medical information or information relating to eligibility for social service or welfare benefits, the disclosure of which would be seen by the average data subject as an especially grievous invasion of privacy.[25]

(h) Is the information unlikely to be accurate or reliable?

The probability that personal data will be accurate may vary quite considerably with the circumstances under which it is gathered or submitted, and the safeguards established or verification procedures adopted by the government institution in question. The likelihood of circulating inaccurate information should weigh against a decision to disclose.

(i) Is there some prospect that the data subject will suffer substantial harm, pecuniary or otherwise, as a result of the disclosure?

Some invasions of privacy may serve not only to embarrass or otherwise diminish the sense of privacy of the individual data subject, but also cause substantial harm of one sort or another. This, again, should weigh against disclosure.

(j) Was the information submitted on the basis of an expectation, tacit or otherwise, that it would be treated in a confidential fashion?

American courts have suggested that, although an undertaking of confidentiality should weigh heavily against disclosure, it should merely be a factor taken into account in determining

whether or not to make the information available.[26] Presumably such undertakings would normally be adhered to but perhaps not, for example, where the individual who initially supplied the information did not rely on the undertaking in any meaningful sense or was in any event required by law to submit the information in question.

No doubt intimate experience with the functioning of freedom of information and privacy protection schemes would enable one to offer further propositions of this kind.

The Ontario Commission recommended a rather elaborate statutory provision[27] in which a number of the foregoing propositions were stated as presumptions to be employed in the application of the balancing test and, I confess, I remain convinced that this is an attractive solution to the problem presented in this paper. At the very least, however, it seems to me that the articulation of principles of this kind should be of assistance to those charged with the task of applying the more vague standards set forth in the American and Canadian legislation.

Privacy is an important but surely not an absolute value, and one which must compete with other values such as that so widely accepted today of the public interest in access to government information. There is a serious danger that the concern to protect privacy will be allowed to submerge the access value, as the virtually wholesale exclusion of personal information from the Canadian Access to Information Act amply demonstrates. It is not too much to suggest the undue deference to the privacy value has substantially undermined the value of the Canadian access scheme. In remitting the question of whether to disclose personal information to the realm of discretionary power, the draftsmen of the Canadian scheme shied away from the task of reconciling these conflicting values.

1. See, Ontario Commission on Freedom of Information and Individual Privacy, Final Report: Public Government of Private People (1980), (hereafter, "Ontario Report), vol. 2, pp. 77-81; J.D. McCamus (ed.), Freedom of Information: Canadian Perspectives (1981: Butterworths, Toronto).

2. Ontario Report, vol. 3, pp. 495-515. See, generally, A.F. Westin, Privacy and Freedom (1967: Atheneum, New York); James B. Rule et al., The Politics of Privacy (1980: New York: New American Library).

3. See, Ontario Report, vol. 3. at pp. 789-798.

4. Canada, Parliament, First Session, 32nd Parliament, 1980, House of Commons, Bill C-43 (An Act to Enact the Access to Information Act and the Privacy Act, to amend the Federal Court Act and the Canada Evidence Act, and to amend certain other Acts in consequence thereof) as passed by the House of Commons, June 28, 1982, hereafter the "Access to Information Act" or the "Privacy Act".

5. 5 U.S.C. Section 552.

6. Id., (b) 6.

7. 5 U.S.C. Section 552a.

8. See, generally, James T. O'Reilly, Federal Information Disclosure (1983: McGraw-Hill, Colorado Springs) vol. 2, pp. 1-38, c. 16.

9. Access to Information Act, sec. 4(1).

10 Id., sec. 41.

11. Privacy Act, sec. 3.

12. Access to Information Act, sec. 19.

13. 424 F. Supp. 847 (1976).

14. Access to Information Act, sec. 42; Privacy Act, sec. 42.

15. D.H. Flaherty, Research and Statistical Uses of Ontario Government Personal Data, Ontario Commission on Freedom of Information and Individual Privacy Research Publication 5, (1979: Government of Ontario, Toronto).

16. Privacy Act, Section 3, (j) to (1) of the definition of "personal information".

17. Cases 2 and 4 are the most problematic. For authorities allowing access, respectively, see, U.S. Department of the Air Force v. Rose, 425 U.S. 352 (1976); Philodelphia Newspapers Inc. v. U.S. Department of Justice 405 F. 2d 670 (DC Cir 1971). In Rose, the requestor sought access to the files with names deleted but the granting of access still offered the prospect of some privacy invasion as readers familiar with the incidents in question would be able to link the files to named individuals.

18. 425 U.S. 352 (1976).

19. Access to Information Act, section 25.

20. 450 F. 2d 670 (DC Cir 1971) of. Masonic Homes v. NLRB 550 F. 2d 214 (3d Cir 1977), (employer denied access to union cards signed by its own employees).

21. See, generally, F.A. Rosenfield, The Freedom of Information Act's Privacy Exemption and the Privacy Act of 1974 (1976), 11 Harv. Civ. Rts. - Civ. Libs. L. Rev. 596 at 611-618; A.T. Kronman, The Privacy Exemption to the Freedom of Information Act (1980), 9 J. Legal Stud. 727 at 767-770.

22. Ontario Report, vol. 2, pp. 332-337.

23. Id. vol. 2, pp. 324-338.

24. 405 F. Supp. 8 (ED Pa 1975).

25. For an attempt at a more elaborate list of such information, see, Ontario Report, vol. 2, p. 338.

26. Robles v. EPA, 484 F. 2d 843 (4th Cir 1973); Washington Post Co. v. U.S. Dept. of Health and Human Services, 690 F. 2d 252 (CADC 1982).

27. Ontario Report, vol. 2, pp. 335-338.

ACCESS TO INFORMATION & BARRIERS FOR PRIVACY: THE SEARCH FOR BALANCE

PROFESSOR T. MURRAY RANKIN *
Faculty of Law
University of Victoria

A. Introduction

Historically, data protection laws and freedom of information laws trace their roots to different sources. They emerged at very different times in European history initially in response to different perceived problems. At present, however, these two separate legal claims have been blurred in many people's eyes. I will argue that this blurring is a consequence of the recent technological achievements which are creating our global "information society". The overlapping of these two legislative regimes may foreshadow the eventual creation of a comprehensive "information law" as our legal rules develop in order to catch up with the advances in computer/telecommunications technology.

Superficially, access to government documents may be viewed as a claim, or perhaps increasingly, as a right in liberal democratic societies; the ability to inspect one's personal files held in government can be seen as simply a subset of this general right of access. Alternatively, the ability to prohibit access by others to one's own information in government data banks is often regarded as the converse of "Freedom of Information".

Laws promoting access to government records originated over two hundred years ago in Sweden. They were passed in an effort to enhance the accountability of the state to its citizens.

Data protection laws, on the other hand, are a comparatively recent reaction to widespread fears about the impact of information technology. As computers and telecommunications come to represent the central nervous system of an inter-dependent world, the manila file folder is being quickly replaced by the computer printout. The printout is being replaced by direct or remote access to government data banks. By Swedish law, for example, citizens are now permitted to use government computers for direct access to government data banks.

Since remote access to government banks is possible beyond one nation's borders, the issue of the transborder data flow of both personal and governmental information has prompted calls for the co-ordination of national laws - in both the data protection and access to information fields.

My central theme is that despite their differing histories, these two legislative fields both represent no more than different tools for individuals and groups of individuals in our society to assist power against the state and against powerful institutions in the state. By some estimates, practically one-half of Canada's gross national product and more than one half of the

---

* Murray Rankin is Associate Professor in the Faculty of Law at the University of Victoria, Victoria, B.C. Professor Rankin has been published extensively on Freedom of Information and is the author of Freedom of Information in Canada: Will the Doors Stay Shut?, published by the Canadian Law Information Council. He is a recognized expert in the field and has testified before Parliament.

employment of our citizens is related to the production, processing, storage and use of information.[1]

To some, the computer is merely a neutral machine; to others, it represents the "infrastructure of tyranny". To still others, like Mr. Yoneji Masuda of Japan's Institute for the Information Society, the near future is keenly anticipated to be a "computopia".[2]

Information "utilities" will permit everyone to obtain information, solve problems and create untold opportunities, merely by connecting one's home terminal to the government "utility".

Whichever prediction proves to be true, most data protection and access to information issues reflect long-standing societal conflicts over the distribution of power, between the state and the individual, the producer and the consumer, and so forth. The computer technology simply speaks a new "language of power".[3]

Sissela Bok summarizes this point in a compelling way: "Conflicts over secrecy - between state and citizen... or between parent and child, or in journalism or business or law - are conflicts over power - the power that comes through controlling the flow of information. To be able to hold back some information about oneself or to channel it and thus influence how one is seen by others gives power; so does the capacity to penetrate similar defences and strategies when used by others. True, power requires not only knowledge but the capacity to put knowledge to use; but without the knowledge, there is no chance to exercise power".[4]

B. Fading Borders

The call for data protection laws reflected a widespread concern over individual privacy. Privacy is an elusive concept. Several years ago, a federal task force on privacy and computers identified three different contexts in which the invasion of privacy may be asserted: (1) territorial privacy; (2) privacy of the physical person and (3) privacy in the information context.[5]

Alan Weston defined this notion of "informational privacy as the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is to be communicated to others".[6]

Until quite recently, the major safeguard of information privacy had been the difficulty in finding particular information stored in a variety of ways in a variety of locations. Today's computers have the speed and capacity to store, combine, retrieve and transfer huge quantities of data very quickly and very cheaply.

Among the O.E.C.D. countries, 9 have explicit data protection laws at the national level (Austria, Canada, Denmark, France, Germany, Luxembourg, Norway, Sweden and the U.S.A.). The United Kingdom's data protection bill will be the tenth such law on the list. Some laws apply only to personal data registers which contain computerized files; some cover manually stored data as well.

Most laws cover personal registers in both the public and private sectors; however, some laws like Canada's Privacy Act, for instance, cover only public sector records. Most such laws protect only personal information pertaining to individuals; some data protection laws, however, such as those of Austria, Denmark, Luxembourg and Norway also pertain to "legal persons" such as companies, societies and foundations. The O.E.C.D. has generated guidelines to help coordinate and suggest maximum data protection standards so that varying national laws do not create non tariff barriers to the flow of data.

Freedom of information laws, on the other hand, now exist in some 10 O.E.C.D. countries, six of which also have data protection laws. Just as the control of one's personal information has generated data protection laws, likewise the accelerating demand for access laws has been part of a larger concern of individuals and groups for a greater degree of control and participation in the government decisions which affect our lives. The ability to participate in an agency's decision concerning the siting of a dam or a hazardous waste facility

or concerning a natural gas rate increase, requires full and timely disclosure of information from government files. Similarly, the ability to see one's complete worker's compensation file or to prohibit others from seeing one's psychiatric records, is essential if an individual is to be more than the passive object of bureaucratic whim. The first set of decisions would be the subject of a freedom of information law; the second, of a data protection regime.

Law reform in both areas fits squarely within a framework of law reform such as liberalized standing rules before courts and administrative agencies, cost awards for public interest intervenors and enhanced "shareholder democracy" within corporations. All of these reforms promote citizen participation.

However, a generalized right to government information clashes with at least four other interests, each of which I will examine in turn: (1) the privacy rights of other individuals; (2) the state's own interest in a core zone of secrecy; (3) the claims advanced by other governments to protect their information in another government's files and (4) the right of corporations to ensure the secrecy of information concerning them which is found in government files.

Firstly, all freedom of information laws contain a cluster of exemptions that seek to defend vital state interests such as national security, law enforcement and coherent policy formation from unauthorized disturbance. The precise scope of such exemptions may differ but the underlying principles do not vary.

Second, all freedom of information laws seek to protect the individual's privacy from all except the individual concerned. When someone requests information concerning another, for example, for epidemiological research, a delicate balancing of judgment is typically required. The U.S. FOIA exempts the disclosure of personal files, "the disclosure of which would constitute a clearly unwarranted invasion of personal privacy".[7] The necessary overlap between data protection and access laws in this regard is perhaps best demonstrated in Australia. Although there is no privacy act at the federal level, an individual may seek access to his/her personal records under the new Australian freedom of information act.[8]

Third, the information provided by one government to another is routinely protected under various freedom of information laws. For example, in both the Canadian Privacy Act and the Access Act, information "obtained in confidence" from foreign governments, international organizations or from the governments of a province, municipality or regional district cannot be revealed by a federal agency.[9] Many departments of the Alberta, British Columbia and Ontario governments, for example, are seeking wholesale protection for their records which are shared with Ottawa. Some access laws like the U.S. FOIA permit access to U.S. nationals and foreigners alike; others like Canada's Access Act restrict use to Canadian citizens and landed immigrants despite the technological ease in retrieving information in public data banks from abroad. At the international level, new challenges to national sovereignty are posed by the new communication technology. For example, how far should one government or multi-national enterprise be permitted to go in collecting sensitive data on another country's natural resources or economic infrastructure? Is there a right of access or a principle of consent which also applies to nation states?

Finally, business enterprises have special concerns about freedom of information legislation. Businesses, too, are concerned that information which they provide to various government agencies be adequately safe-guarded. But can a corporation have "privacy"? Sissela Bok answers 'No':

"Claims of privacy are often made for (practices of large-scale collective secrecy such as trade secrecy) and the metaphors of personal space are stretched to apply to them. To be sure, such practices are automatically private in one sense, so long as they are not

public. But the use of the language of privacy with its metaphors of personal space, spheres, sanctions and boundaries to personalize collective enterprises should not go unchallenged. Such usage can be sentimentalized as the excessive resort by poets to the "pathetic fallacy" (in which personal feelings such as grief or cruelty are ascribed to nature) and can thus distort our understanding of the role of these enterprises".[10]

Therefore "privacy" claims advanced by corporations are really an assertion of property rights or assertions of power vis-a-vis the public or nosy competitors.

Although corporations are not given status under the Canadian Access Act, their principals or lawyers may seek information for themselves or as part of a campaign of what Americans have termed "industrial espionage". Just as with individual privacy, a delicate balancing judgment is required under an exemption in the Access Act in order to protect confidential business information from wrongful disclosure.[11] Business information which is otherwise confidential may be disclosed "if such disclosure would be in the public interest as it relates to public health, public safety, or protection of the environment and if such public interest in disclosure clearly outweighs in importance" the business interest asserted.

Interestingly, however, greater rights in this regard are provided to business interests than to individuals in the Canadian legislation. Under the Access Act, business enterprises are given the explicit right to be informed in writing of a possible disclosure of their information. They also have the right to contest such disclosure all the way to the courts in what the Americans call "Reverse FOI Suits".[12] However, the Federal Government may release sensitive personal information to a wide array of third parties without the individual's knowledge or consent - subject only to oversight by the privacy commissioner in certain instances.[13]

The ability of business enterprises to enjoin others from gaining access to their information found in public sector data banks is a substantial countervailing power for our corporate sector. Professor Christan Bay, however, would extend the principle of openness and accountability which freedom of information laws seek to foster in the public sector to the private sector as well. Prof. Bay advocates a right of access to the information held by all private companies operating in the public domain in light of the power these institutions exercise over our lives.[14] His suggestion is consistent with the increasing development of participatory shareholder democracy in the United States.[15]

C. Conclusion

Both data protection and general access to information laws are examples of a trend in the Canadian legal culture toward the codification of procedural entitlements. The charter of rights and freedoms is another prominent example of how an increasingly heterogeneous society like ours has begun to require that certain procedural entitlements be made explicit. Entitlements which in most cases were implicit in the past have now become constitutional rights. This trend may reflect an increasing distrust of large institutions by ordinary citizens, perhaps fueled by a fear that personal privacy and similar values are being eroded by the computerized infrastructure of our complex society. As this information society develops, a comprehensive and international framework of "information law" must also develop, with all the balancing judgments discussed above likewise made expicit.

In my view, the emergence of these new kinds of procedural rights to information - personal, governmental and even corporate - should be understood as a contemporary application of what Justice Frankfurter said many years ago; "The history of (American) freedom is in no small measure the history of procedure".[16]

Thank you.

ENDNOTES

1. This figure is quoted from R. Grant Hammond, "Quantum Physics, Econometric Models and Property Rights to Information" (1981) 27 McGill L.J. 47 at 48.

2. Y. Masuda, The Information Society as Post-Industrial Society (Tokyo: Institute for the Information Society 1980) at 114, 146.

3. H. Burkert, "A Functional Explanation of Data Protection Laws" (1982) Computer L.J. 169.

4. S. Bok, Secrets (New York: Pantheon Books, 1982), p.19.

5. Canada, Department of Communications and Department of Justice, Privacy and Computers (Ottawa: Information Canada, 1971) at p. 13-14.

6. Alan F. Westin, Privacy and Freedom (New York - Athenum Press, 1967) at p.7.

7. USCA S.552 (B) (6).

8. S. 41 of the Australian Freedom of Information Act exempts documents the disclosure of which would involve "the unreasonable disclosure of personal information". However, Section 41(2) states that this does not affect an individual's request for access to one's own information. Section 45 also exempts the disclosure of information that "would constitute a breach of confidence", which has also been interpreted to safeguard personal privacy. Recently, the Australian Law Reform Commission recommended the passage of a Privacy Act to clarify the scope of informational privacy and to extend the right of access to the private sector, starting with the Australian Commonwealth Territory.

9. S. 19 Privacy Act; S.13 Access to Information Act.

10. S. Bok, op. cit, supra note 4, at p. 13-14.

11. See S. 20 (6) Access to Information Act.

12. The first case decided under the Access to Information Act raised just this kind of issue: Maislin Industries Ltd. v. Minister of Industry, Trade and Commerce et al (Federal Court, Trial Division per Jerome, A.C.J. May 9, 1984).

13. Section 8(2) of the Privacy Act sets out 13 wide categories in which the disclosure of personal information to third parties is authorized.

14. C. Bay - "Comment", in J.D. McCamus, Freedom of Information: Canadian Prospectives (Toronto: Butterworths, 1981), p. 23

15. See discussion in John Naisbitt, Megatrends (New York: Warner Books, 1984), p. 197.

16. Malinski v. State of New York (1945), 324, U.S. 401, 411, (Frankfurter, J.)

CANADIAN PRIVACY LEGISLATION IN COMPARATIVE PERSPECTIVE

PROFESSOR DAVID H. FLAHERTY *
Privacy Project
University of Western Ontario

My object is to make some comparative comments on privacy and data protection laws. It is a difficult task, in part because the audience contains a number of people who are experts on various aspects of the subject. We are all very pleased to see others in this audience bringing a new interest to the subject of protecting privacy, something that has been a late bloomer in Canada, certainly at the provincial level and in the private sector.

My main research interest is not simply trying to promote laws on privacy and data protection but in seeking to make them effective once enacted. This is an odd position to take in Canada because we are all well aware that there are nine Canadian provinces that do not have such legislation, even though I think it is admirable that the Honourable Norman Sterling is going to introduce a Privacy and Access Bill in the Ontario legislature tomorrow. Canadians keep thinking that they need to invent the wheel in order to do wonderful things, but in fact we are behind most of the Western world in data protection achievements, which is perhaps a useful point to make in beginning this presentation.

Most of my comments are directed to the public sector, simply because I believe that data protection legislation is needed first there. I happen to think that the private sector can pursue voluntary self-regulation for the moment and that it is incredibly presumptuous for the provinces (except for the province of Quebec) to be talking about regulating the private sector when they have not put their own houses in order by passing public sector data protection laws.

I know it is not the fault of either my panel colleague, John McCamus, who was Director of Research for the Williams Commission, or of the Minister, Mr. Sterling, that legislation has not been introduced before now in Ontario, but it is clearly about time that Ontario passed a data protection bill. Let me emphasize the point by reporting something about such developments in foreign countries. I will proceed from the most to the least effective laws, except for Canada, which is in a separate category at the end of my presentation.

West Germany has had a federal Data Protection Law since 1977 and counterpart state legislation. They are very effective statutes. The Germans have a

---

* David Flaherty is a Professor of History and Law at the University of Western Ontario in London, Canada. He is an internationally known expert on personal privacy and is the author of Privacy and Government Data Banks. An International Perspective (1979), as well as many other studies. He is currently completing a three-year research project on how data protection laws for the public sector are working in practice in six countries.

co-ordinated system of data protection laws for the public sector and for the private sector, although the private sector regulation is relatively weak, because it is primarily self-enforcing. Instead of each of the eleven states passing their own novel law, all of the statutes look much the same, so a citizen wishing to exercise privacy rights is looking at relatively similar legislation. One prays, although it is unlikely to happen, that such rational coordination will occur in Canada, following the model of the federal Privacy Act of 1982.

The powers of the various Data Protection Commissioners in West Germany are advisory only, which I happen to think is very desirable; such power is comparable to that of our federal Privacy Commissioner. Data protectors do not really need pervasive regulatory powers; in Sweden and France, and in the proposed U.K. Data Protection Bill, such strong powers result in an incredible amount of bureaucracy and in relatively ineffective implementation of data protection, because of the paperwork burden.

Another important trait of the Federal Data Protection Commissioner's office in West Germany is that it has a very talented and dedicated staff. I am finishing a book on the subject of what makes data protection laws effective, and one really critical factor is who serves as the Privacy Commissioner or who heads up the Commission or the Data Inspection Board.

Moreover, if such leaders do not have really good staff, data protection can be just a form of window dressing. The state of Hesse has more than six million people and is thus comparable to Ontario, for example, in terms of population. Hesse has a very distinguished Data Protection Commissioner, Professor Spiros Simitis, who is also a major international influence in this field.

One problem in Hesse is that there are only ten staff people to implement data protection for the entire public sector. There is a tremendous risk of the staff simply being overwhelmed by their statutory tasks of regulating the collection, use, dissemination, and storage of personal information. It is really a very overwhelming kind of situation. Simitis prides himself in being non-bureaucratic and in having a small staff. But the staff complain that they cannot do the work and acknowledge the risk of offering only the illusion of data protection. The worst offense is to pass a Privacy Law and then not really implement it in an effective way in the public sector.

The Germans are notable in data protection for carrying out inspections. Over a period of time, they actually visit personal information systems, audit the computers and the information that is being collected, and learn what is being done with it and how it is being transferred. This important inspection role is better done in West Germany than anywhere else in the Western world where data protection laws exist for the public sector.

I would also emphasize the importance of the fact that these West German Commissioners are all very independent individuals under the law, so independent in a way that when Professor Hans Peter Bull, the first Federal Data Protection Commissioner, came to the end of his five-year term, he was not re-appointed by a newly-elected conservative government, after having carried out effective data protection, particularly in the police and security fields.

There is also enormous controversy in Ontario over the law enforcement implications of Privacy and Access to Information laws. Yet the West German federal and state police have learned to live very well with data protection, after some initial shouting and screaming at one another. Germany has much more sensitive security issues, especially with the terrorist activity it has had in the last ten years, than we have in Canada; yet data protection has been implemented in the three security agencies, which seems surprising to the English-speaking world.

Some of the concern for law enforcement interests that emerged in connection with Bill C-43 at the federal level and that we are now seeing in Ontario is

really misplaced. The police in other countries have learned to live with data protection and privacy legislation; I should also acknowledge the success of the RCMP at the federal level in this country in learning to live with data protection. West Germans use a very collegial and non-adversarial approach to making data protection effective, which is a critical characteristic of good privacy and data protection activities.

I have time only to note that data protection is very controversial in Sweden. My view is that if data protection activities are not controversial in the public sector, then the Privacy Commission or Data Protection Commission is not really doing his or her job. These officials are given independence in order to articulate privacy interests on behalf of the general public; it is one of the primary activities of an oversight agency.

The French have an extraordinary data protection law, but they have not done much about implementing it. The law of January 6, 1978 created a very unwieldy seventeen-member Commission Nationale de L'Informatique et des Libertes (CNIL), who are part-time people. They have not done much in their first five years; moreover, they have had a very weak staff.

The CNIL now has a new president who is turning his attention to some of these matters, and there is a likelihood that it will become a somewhat less politicized and somewhat more effective agency. It is desirable that the new President of the CNIL, M. Jean Rosenwald, is not a politician, because I do not think an active politican has functioned very well in that particular post in the past.

In its first five years the CNIL has demonstrated a lack of political will to resist the government on significant issues concerning the creation of new information systems. The French situation specifially illustrates the risks of an agency of this type providing only an illusion of data protection rather than the reality, particularly in the public sector.

The U.K. has a new Data Protection bill, which is discussed in detail elsewhere in these proceedings. We have been waiting for this bill for more than ten years. Now it looks like it will be enacted into law in the next month or two. I believe it is much too bureaucratic a law because of the paperwork involved. The British are registering users of personal information rather than uses; the latter is the normal way of proceeding.

It is estimated that there are over 200,000 users; past experience would indicate that there are probably many more. The Data Registrar will have a staff of twenty to thirty persons. The Registrar is going to have to be a superman or a superwoman to do the tasks assigned. The selection of the Registrar will be critical to the success of the legislation, since the person chosen will have to work extremely hard to make the legislation effective.

When we look at the U.K. bill from a North American perspective, it is an extremely powerful piece of legislation, because it requires all holders of personal information, both in the public and private sectors, to register and to comply with certain rules and regulations which have the force of law, including civil and criminal sanctions for breach of the principles of fair information practice. From a perspective within the U.K., some critics regard the bill as reasonably weak; the Registrar in fact does not have much power to do anything. You should be aware that within the U.K. there is considerable criticism of the inadequacies of the bill, in that it does not cover manual records, for example.

About the United States, I will simply note that there is a federal Privacy Act of 1974. It's fundamental inadequacy is that it does not include a Privacy Protection Commission, an oversight agency that would, on a continuing basis, articulate privacy interests against competing forces. It is primarily a self-enforcing law; where you do not like something, you have to go to court as an individual to enforce your privacy rights at the federal level, which has proven to be a very ineffective way of doing business.

One of the consequences of the lack of a Privacy Protection Commission is that such novel practices as computer matching of miscellaneous personal records are out of control in the United States. On the other hand, the United States does have strongly developed constitutional rights to personal privacy, which we do not yet have in Canada. The California constitution, for example, acknowledges the rights of citizens to enjoy personal privacy. Finally, New York state has passed a Personal Privacy Protection Law which goes into effect on the 1st of September of this year. What is important is that it includes an oversight agency, the Committee on Open Government, whose task is to make sure that the law is working in the public sector.

Turning to Canada on this quick tour, I like the federal Privacy Act. The role of the federal Privacy Commissioner is well-defined. Without in any way casting any aspersions on the incumbent, Dr. John Grace, when I reflect on a law that has only been in effect for eleven months, I am reminded that a Privacy Commissioner and his staff need to be activists in order to make data protection effective. You have to make inspections of government agencies in order to find out what is really happening in terms of the collection, retention, and use of personal information by the federal government.

I happen to believe, and I am more than a little perverse in this perspective, that all of the emphasis on rights of access by individuals to their records under the Privacy Act is misplaced. In fact, it is not the most important activity in the Western world, even though in Canada we have tended to emphasize that aspect of Privacy and Access to Information. I really believe that the staff of a Privacy Commissioner must learn what records actually exist, question the existence of records, if necessary, and help to destroy unnecessary personal data, in order to make data protection effective.

I want to highlight the fact that Quebec is the only province in Canada which has public sector data protection with its Law 65. The Quebec Commission d'access a l'information is one of the most powerful regulatory commissions that I have ever encountered in this field. It has oversight over 3,600 public agencies, including schools and hospitals. It has considerable administrative power to establish the criteria for the collection, use, retention, and transfer of personal information. Law 65 enters into full effect on the 1st of July of this year. My fear is that the modified French model that is being used in Quebec is going to be much too bureaucratic to be effective, that the Commission is simply going to be overwhelmed with paper, even though I applaud the fact that the choice of Commissioners has been extremely good. In the first instance only one of the three Commissioners is a lawyer, and two of them are women, which I regard as twin forms of progress.

I would like to close with a list of ten commandments about data protection. I can hardly give you the rationale for each of these points here, but it will recapitulate the finding of the tour I have been giving you.

It is an absolute necessity to have privacy and data protection laws for the public sector and for sensitive applications of personal information in the private sector. One of the fundamental inadequacies of most such legislation, at present, is that it does not adequately define the privacy interests that are supposed to be protected by such legislation. Most of the laws simply assume that privacy is a good thing, but make no effort to tell you exactly what this privacy business is that is supposed to be protected. Society places considerable power in the hands of civil servants, and there is always the risk of Data Protection Commissioners or Privacy Commissioners exceeding their mandates.

I further believe that Privacy Commissioners and data protection agencies should concentrate on data protection. No such commission in the Western world has more than thirty-five staff. Although such anti-bureaucratic tendencies are desirable, the risk is that the staff are simply going to be overwhelmed

by their tasks and are not going to be able to do the things that are necessary. So they should not be intimately involved with all of the questions of information law or information policy that, in many ways, they are well qualified to treat. The protection of privacy in the public sector is so important that data protectors should basically stick to that task.

You cannot have successful data protection laws without data protection agencies. I am pleased that in Ontario Mr. Sterling is talking about the creation of a Data Protection Office, but I find it perverse to be proposing a Data Protection Office separate from that of the Privacy Commissioner. This is another "unique" Ontario initiative that I find dubious. The task of data protection is difficult enough without creating two separate offices.

It is extremely important that Data Protection Commissions be organized in an effective manner. It may seem simple minded to make this point, but it is a critical issue, based on the experience with implementation that I have observed to date. The quality of people who actually help the Commissioners do their work is really going to make the difference in the long run.

The independence of the Commissioners is also critical. In almost every country, these extraordinary Privacy Commissioners, if I may simply call them that, have been given a considerable degree of independence from the government, because the work they are doing is so important. In almost every instance such status is a unique constitutional position, which is essential to the successful conduct of data protection.

I also believe in advisory powers for data protectors as opposed to strong, regulatory capacity to issue commands. I really think that privacy is to a considerable extent a vague and inchoate concept, that protecting it really should be a matter of balancing interests and of debate back and forth among the regulators and the regulated. Given the small size of the agencies, the process of implementation needs to have an "advisory" character in order to make data protection effective.

Among the important powers of a data protection agency is the capacity to receive complaints from citizens, which will be few and far between, but will nevertheless alert the agency about areas that the public are concerned about.

It is also necessary to have the power to carry out audits and inspections of personal information systems. The Data Protection Office in Ontario should be examining the O.H.I.P. system, should be finding out what is actually happening in the welfare systems, and should really contest, debate, and question the retention, collection, use, dissemination, and transfer of personal information by government agencies.

Data Protection Commissioners also have a fundamental obligation to pay a lot of attention to evolving information technology, even though I sometimes believe that information technology is so far ahead of the regulators that there is not much chance of them catching up anyway. The kinds of world information networks for personal information that already exist are in many ways already far beyond national regulation; one need only look at the world wide information networks of the Canadian chartered banks. Nevertheless, data protection agencies have the responsibility to monitor these developments and to alert the politicians and revisors of their legislation as to the real state of play in this connection.

Finally, it is my view that the ultimate task of the Data Protection Commissioners is to develop specialized protective legislation and regulations for each type of personal information system.

It is all very well to have a general federal Privacy Act, but we should now be working on improving specific provisions on confidentiality and data use in, for example, the Income Tax Act, the other federal statutes on personal information, and, ultimately, in such private sector legislation as the federal Bank Act.

Thus, making data protection effective in the public sector in Ontario will be an enormous task, even if legislation is enacted that can stand comparison with the accumulated experience of the last fifteen years in other countries.

Editors Note: Unfortunately, the President of CNIL, M. Rosenwald, referred to on Page 69, died on June 2, 1984. His successor as President is M. Jacques Fauvet.

PANEL 3: PRIVATE SECTOR PANEL: "PRIVACY: WHAT THE PRIVATE SECTOR HAS DONE"

CHAIRMAN: Professor David Flaherty *

PANELISTS: Ralph Hancox

Robert G. Logan

Eric Wimberley

COMMENTATOR: Mel Fruitman **

---

* David Flaherty is a Professor of History and Law at the University of Western Ontario in London, Canada. He is an internationally known expert on personal privacy and is the author of Privacy and Government Data Banks. An International Perspective (1979), as well as many other studies. He is currently completing a three-year research project on how data protection laws for the public sector are working in practice in six countries.

** Mr. Fruitman is the Research Manager of the Retail Council of Canada. He is also Vice-President of the Payment Alternatives Communications Exchange (P.A.C.E.). This organization was formed in 1982 and its objectives include: promoting co-operation among sectors such as retailing, banking, equipment suppliers, telecommunications carriers and consumer representatives; exchanging information; representing the interests of members in electronic funds transfer and point of sales (EFT/POS); promoting standards leading to compatibility for an EFT system; clarifying members' needs; maintaining liaison on EFT/POS developments; and encouraging the development of EFT/POS in Canada.

MAILING LISTS AND DIRECT MAIL MARKETING

RALPH HANCOX *
President
Reader's Digest Association of Canada, Montreal

At the outset, it might be useful, to put the privacy issue into perspective so far as direct mail marketing and mailing lists are concerned.

Unsolicited mail has a high profile in some quarters and, according to various indignant consumer protection spokesmen who have voiced opinions on the subject, a high irritation factor also.

Of the total mail volume delivered by Canada Post in recent years - about six billion, four hundred million pieces annually - some fifty percent, or three billion two hundred million pieces, fall into this category.

This approximates an average of a little less than two pieces of unsolicited mail (including bills) per household per delivery day. It is axiomatic that Canada Post would like to increase this average since this class of mail is, by virtue of its pre-sorted, batched characteristics, the most profitable kind of mail packet to handle.

It should also be said that, in Canada, direct mail marketing is an undeveloped sales technique. In a comparison with the United States our volumes are easily less than one twentieth of theirs per capita.

A variety of countries have tested public opinion on the subject of intrusion by mail and, it is true, there is a portion of the general public that would class unsolicited mail as an 'invasion of privacy'.

This small body of opinion also responds favourably to the sobriquet 'junk mail' which is applied by critics to unaddressed mail packets.

But when the privacy issue of mail delivery is tested on the spectrum of substantive privacy issues such as :

Would you regard it as an invasion of privacy if:

- one department of government made personal data from your file available to another government department?
- you were required to carry an identification card bearing your social insurance number?
- your neighbour allowed her dog to defecate on your lawn?
- you were regularly approached by door-to-door sales personnel to buy unsolicited merchandise?

---

* Mr. Hancox is a graduate of the School of Modern Languages, London, England and a Harvard Nieman Fellow (1965-1966). He is President of The Reader's Digest Association (Canada) Limited. His interest in legislation concerning data protection arises from the implications for direct mail marketing, list management and the consequences of the large computer configurations required to conduct business operations today.

- you were asked to supply personal information over the telephone to a caller not known to you?

unsolicited mail as a privacy issue becomes of negligible concern.

Similarly, on the question of mailing lists and the renting of names (which has been criticized in some quarters as an invasion of consumer privacy) public indignation - which in any case has never been high on this subject in North America - becomes inconsequential in the face of such questions as:

> Who would you wish to intercept, or prevent the delivery of, unsolicited commercial mail destined for delivery to your household:
>
> - the government?
> - the post office?
> - an independent agency?
> - an industry association?
> - the police?
> - none of these?
>
> Would you prefer to do it yourself?

When the question is asked:

> Would you object if a
>
> - charitable organization,
> - commercial enterprise,
> - local merchant,
> - direct mail marketing organization,
> - magazine publisher,
> - social club,
> - health and fitness organization,
> - government department,
>
> took your name and address from a telephone directory
>
> to solicit your support,
> to ask for a donation,
> to offer goods or services for sale,
> to distribute information?

the answer reveals a very low level of anxiety in respondents about mailing lists.

It goes without saying that the weight of these answers can be very rapidly altered by phrasing questions to introduce the concept of the direct mail marketing, or delivery, of pornographic or other material generally regarded as offensive or unsolicited material to children.

There is a further change of attitude when the unknown mailer uses information which is quite clearly personal in nature.

> 'In your garage you have a brand new Ford... would you like a set of seat covers... '
>
> 'You, your husband and three children will be delighted with... '

Such approaches immediately raise the questions:

> 'How did they know... ?'
>
> 'Where did they get my name and address... ?'

Those who compile mailing lists, and those who send unsolicited sales promotions to addresses on such lists, have a common interest in limiting and guaranteeing the information involved.

Such lists should contain up-to-date addresses - that is to say, people on them should be at the address stated. They should also be among those who have a high probability of responding to unsolicited mail. They should not contain names and addresses of people who object to unsolicited mail, or who have died.

It is expensive to plan, direct and control a mail marketing campaign. The efficiency of the response levels is crucial to profitability.

Thus mailers share with recipients a desire not to send mail to those who genuinely do not want it. (The question of sending unsolicited merchandise and then billing for it is, or course, another question already covered in consumer legislation.)

The question, always, for the mailer is how to avoid sending material to those who will never respond.

One way of increasing the probability of response and increasing response levels of mailing lists is to compile historical information on buying patterns and preferences of individuals on that list and to code lists with demographic and other sociographic information.

Such information can be weighted and regression formulas can be applied to name selection. In such a process, each name on the list to be regressed would receive a score. Only those names whose scores exceed a certain level would be selected from the list to mail.

The more accurate the regression, the more closely a direct mail marketing campaign can approach the nirvana of mailing only to those who respond favourably.

In fact, as the state of the art now is, a reasonable response level is a low percentage, normally well below ten percent. An acceptable improvement from regression would be a one percent or even .75 percent increase in response.

The percentage of respondents, depending on a variety of factors, may be always in that order of magnitude for a particular list, but the individuals in that list who respond on successive occasions will be randomly distributed throughout the universe and may seldom respond twice to repeated mailings.

The notion, therefore, that direct mailers can - or would want to - make sinister use of information on mailing lists, or any use except to increase the response level, is highly fanciful.

The issue of intrusion is also raised in discussions of unsolicited mail and, should, perhaps, be disposed of in this attempt to set the perspective.

Direct mail marketing is, among selling methods, a low pressure sales technique, the initiative for which, after the first mailing piece has been dispatched, is always in the hands of the buyer. Consider the following:

A potential customer receives a mailing piece. The customer can decide to open the envelope or discard it.

If the customer opens the envelope, the contents will either prompt an order or be discarded.

If the customer places an order, the order must be put in an appropriate envelope, be stamped and be mailed, giving time for further reflection.

If the order is mailed, the customer will receive the goods ordered and may accept them, hold them for a trial period or return the goods to the merchant.

Then, of course, comes the task of billing and payment. The merchant trusts and prays that the payment response level matches the original response level for orders.

Three points are of interest to conclude this part of the discussion:

1. In places where an opportunity exists for consumers to remove their names from mailing lists, not many people do so (in Canada, some 27,567 people or some .34 percent of the active households have registered with the Canadian Direct Marketing Association for this purpose).

2. Significantly more people ask to be put on mailing lists than ask to be taken off in the American experience.

3. The trading of mailing lists which are up-to-date and which are marked with data already in the public domain - such as address and postal code - is an economic benefit to the industry and the consumer. (So much so, incidentally, that a state advisory committee concluded in Illinois that 'the sale of driver license lists by a government unit to direct mail firms does not constitute an invasion of privacy' and that it should be encouraged by legislation.

That same committee made another point which neatly leads into the next body of issues to be considered.

In a discussion of whether applicants for a driver's license should have the option of excluding, by check-off, their names from the list that the State of Illinois could trade, the committee reported thus:

> 'We have examined the practical effects of... granting an option... to preclude the Secretary of State from disclosing information as to applicant's name, address, date of birth, and other related information... The objective of the check-off would be to protect persons from the receipt of unsolicited mail. We find that the check-off would not achieve the objective sought... The likely result would be that the Secretary of State would be criticized for misleading persons and not preventing the delivery of unsolicited mail...'

This comment is very true. As the Australian Law Reform Commission found when it examined the whole issue of privacy in all its aspects. It quotes the following passage in support of its recommendations on mailing lists:

> 'If an individual does not want to receive unsolicited mail, he can keep his name off most lists by becoming a modern-day hermit - by paying cash for all his purchases, not owning a car, giving to charities anonymously, always buying magazines at newsstands, never responding to door-to-door surveys, never signing a petition or guest book, never registering to vote, never attending a meeting or conference, or newsworthy or social event... even so he may get a certain amount of unsolicited mail addressed to the occupant.. '

Here, the author has chosen to interpret the individual as a male. We are all aware that, in the same household may live a male and a female who have differing views on whether that household, or one of the occupants of it, should be on, or off, mailing lists.

In the discussion of various legislative models contained in the discussion paper circulated at this conference the registration of mailing lists is reviewed.

When Sweden took this approach it expected registrations at barely one hundred such lists; its registration office, however, was swamped with applications for thousands.

This is very understandable. An enormous number of lists are compiled for the purposes of mailing information to various universes. Clubs do it, schools do it, even mothers and politicians do it.

And in a communal society, it is very desirable that we <u>do</u> do it because it is all part of the network of the free flow of information.

As we have already noted, it is in the interest of the commercial mailer to ensure, as far as is possible, that the names on the list to be mailed are favourably disposed towards the mailing, contain only information which will enhance the efficiency of that mailing, are up-to-date and are judiciously used.

In a study commissioned for the Council of Europe, John Braun made this observation:

> 'If it is accepted that the use of the mail is open to anybody --- list or no list --- and that what is relevant is the <u>content</u> of the mailing piece and not the act of mailing, then the issue to be faced is one of detriment. Is there anything in the content of the mail which offends against fair trading, honesty, morality, taste or any of the many possible alternatives? If the respondent is misled or likely to be misled or defrauded or shocked by the nature of the communication, there is cause for intervention by the appropriate authority'.

In most jurisdictions, such matters are already covered in legislation or regulation. What is not always covered and which, in the growing opinion of observers, <u>should not be</u>, is the registration,

content, or use of commercial mailing lists.

The reasons, most generally are those of cost and impracticability.

The further and most powerful reason, of course, is that the process of self-regulation is in the best interest of users, society and recipients, in any case.

This does not imply that there are no abuses and no weaknesses and no faults where self-regulation is applied. There are; but these can be shown to be far less than those which would occur and have occurred in legislatively regulated systems.

Consider, for example, the anomaly in a jurisdiction, where it would be illegal to publish the sex or political affiliation of members in a list of names and addresses of the constituents of a legislative assembly. This sort of thing is one of the hazards of an overzealously worded privacy regulation.

Less far-fetched, but equally absurd, would be a requirement for clubs, say, to register their lists of members, and submit the information contained on such lists for approval, by club members. This regulatory precaution would be against the eventuality that the list might be rented or sold to a commercial enterprise with a legitimate interest in mailing the people on it.

The Organization for Economic Cooperation and Development has published guidelines governing privacy protection where mailing lists are concerned and these have been widely embraced. The U.S. and Canadian Direct Mail Marketing Associations and marketing groups in European, British and Scandinavian countries have all adopted codes of conduct and it is of interest that such actions have taken place in countries where legislation is in place and where it is not.

Essentially, all these codes embrace the following principle and concepts contained in Reader's Digest's code.

1. Personal data collected and stored are limited to those relevant to the efficient marketing, order processing, servicing, billing and collection of payment for the company's products and services, and are used only for these purposes.

2. The personal data files are frequently updated with new information to ensure that they are accurate, complete and current.

3. Reader's Digest responds on a timely basis to written requests from Customers or other individuals (or their documented legal representatives) for summaries of their personal data in the file. Personal data shown to be inaccurate, obsolete, or incomplete are corrected.

4. Except for debt recovery purposes on behalf of Reader's Digest or when required by law, personal data are not released to third parties.

5. Strict security procedures are maintained to protect against unauthorized access, destruction, use, modification of disclosure of personal data on Reader's Digest Customers.

6. Reader's Digest supports efforts of industry associations to which it belongs to encourage the disclosure of list rental or exchange policies and the offer of a name removal option by companies who engage in those practices.

7. Reader's Digest honors on a timely basis all requests from those who do not wish to receive its promotional mailings by appropriate notation to the file. The requests may be received directly or through third parties, such as consumer and industry associations or government agencies.

8. Reader's Digest complies with all local laws and regulations relating to data protection and privacy.

Reader's Digest does not rent or trade the names and addresses of its customers, incidentally.

Progressive companies are increasingly adopting well formulated and responsible voluntary codes, which, if they contain such elements as those outlined in the Discussion Paper circulated for this meeting would render anything but an umbrella statute unnecessary.

Along these lines, the Australian Law Reform Commission, in its recommendations has struck the right balance. It is perhaps, worth repeating the essential elements of a worthwhile code on list management to bring this presentation to a close.

- Personal information should be obtained and processed fairly and lawfully;
- Personal information should be held for a specified and legitimate purpose or purposes;
- Personal information should not be used or disclosed in a way incompatible with those purposes;
- Personal information should be adequate, relevant, and not excessive in relation to the specified purposes;
- Personal information should be accurate and, where necessary, kept up to date;
- Personal information should be kept in name linked form for no longer than is necessary for the specified purposes;
- The data subject should have access to information held about him or her and be entitled to its correction or erasure where the legal provisions safeguarding personal data have not been complied with;
- Appropriate security measures must be taken against unauthorized access, alteration or dissemination, accidental loss and accidental or unauthorized destruction of data.

It is self-regulation that prompted the Australian law commission on reform to conclude:

'The commercial benefits arising from adoption of these methods (which I described earlier) by direct mailers (in particular, reduced cost of mailings improved returns, enhanced customer goodwill) provide motivation to members to pursue these schemes. This facilitates market advantages of the direct mailing system, which includes increases in sales of goods and services and expansion of employment proposals, while minimizing the number of people receiving unsolicited communications...'

PRIVACY BEGINS AT HOME

ROBERT G. LOGAN *
Director, External Programs
IBM Canada Limited

The foundation for IBM's practices on privacy began with employee privacy and is based on the company's principle of "Respect for the individual". The company has always recognized the need for positive employee relations and consequently focussed first on employee information practices long before privacy itself became a public issue. Moreover, because of the nature of its business, IBM as a computer manufacturer believes that it has a special responsibility to establish and maintain unusually high standards, not only with respect to data security but in the way it manages personal information about its employees as well.

Hence, at IBM we believe that "Privacy begins at home". Indeed, "home" is wherever personal information is being handled.

Therefore, the protection of information and data security is best accomplished by the users after consideration of the particular environment, the need for protection, and the purposes of the data.

Inherent is such a decision is defining two terms which are often confused - privacy and data security. Although they are closely related, there is a distinct difference between the two. We believe privacy to be a socio-legal issue concerning the kinds of information held in record-keeping systems and the purposes for which the data is used. Data security on the other hand is a technical and procedural issue concerning the control and protection of information. The two terms should not be used interchangeably.

Privacy is an old concept which focuses on the protection of information, while data security is a relatively new concept relating to the integrity of record keeping or filing and quite often is resolved by a mechanical solution.

Privacy can conflict with other fundamental rights - for example - freedom of information.

Privacy therefore, becomes a balance between limiting access to information to protect privacy and allowing freedom of information in the public interest, thus permitting users of information to meet the needs of society and to provide good and efficient services.

What is the role of the private sector in responding to the privacy issue and does it differ from the public sector? I will return to this but first let me tell you about our experience with privacy.

At IBM, fair information practices have evolved over a long period of time - almost 20 years to be exact. Of course, concerns regarding privacy preceded both IBM and the advent of computers. Writ-

---

* Mr. Logan is the Director, External Programs, for IBM Canada Limited. In this capacity he is responsible for identifying and analyzing factors and trends of a political, social or environmental nature which could have an effect on IBM's business. He is very active in community and national affairs including memberships in the Canadian Club, Empire Club and the Canadian Chamber of Commerce.

ing in the Harvard Law Review in 1890 Louis Brandeis warned of "mechanical devices" that would threaten the solitude and privacy of individuals. Because of a cluster of new inventions, he noted, a "next step" was needed to protect a person's "right to be left alone". That warning went largely unheeded and the mechanical devices he wrote about so warily -- the camera and the telephone -- quickly passed into familiar use and abuse.

Computers simply increased the concerns of those who would protect the individual from the misuses of technology. IBM Chairman, Frank Cary, stated in the Harvard Business Review in 1976:

> "Organizations have invaded people's privacy with steel filing cabinets and manila folders for years. But computer systems with remote access have intensified both the problem and the public concern."

IBM believed that the way to take some leadership in this area was to clarify its own position regarding employee privacy in personnel recordkeeping.

This issue actually dates back to the 1960's in IBM when an employee requested to see his personnel folder and was refused by his management in accord with company practices at the time. The issue was reviewed and practices were changed making provision for employees to review their personnel folders.

In 1971, IBM commenced a study of the status of employee data within the company culminating in the publication of four principles of privacy in 1974 which were nationally advertised in magazines and newspapers;

1. Individuals should have access to information about themselves in record keeping systems. And there should be some procedure for individuals to find out how this information is being used.

2. There should be some way for an individual to correct or amend an inaccurate record.

3. An individual should be able to prevent information from being improperly disclosed or used for other than authorized purposes without his or her consent, unless required by law.

4. The custodian of data files containing sensitive information should take reasonable precautions to be sure that data are reliable and not misused.

Also, in 1974, IBM commenced a management training program on employee privacy. Discussion ranged from an employee's right to ask questions about what is in the personnel file to the propriety of telephoning or visiting employees at home. As a result of these training programs, many privacy-oriented issues arose and many changes in practices and procedures were implemented. Privacy became a part of the fabric of every IBM manager's job.

In 1975, IBM published a newly developed set of practices for managing employee personal information and distributed this to all employees:

1. Collect, use and retain only personal information that is required for business or legal reasons;

For example, data no longer included on employment applications are: birth date, spouse's employment, relatives employed by IBM, military service, and previous addresses.

Furthermore, while it is traditional to publicize employee promotions, reassignments, awards and other achievements, employees are now asked beforehand if they agree to such publicity.

2. Provide employees with a means of ensuring that their personal information in IBM personnel records is correct.

The core of IBM's effort to ensure employee records are both accurate and fair is that its practice o open access with relatively few exceptions such as personnel planning data, permits employees to see and correct files containing information about themselves.

3. Limit the internal availability of personal information about others to those with a business need to know.

For example, the employee's manager does not have access to such things as payroll deductions, medical records and selected employee benefits.

4. Release personal information outside IBM only with employee approval, except to verify employment to satisfy legitimate investigatory or legal needs.

For example, without written approval, the only information IBM will release outside the company about an employee is for employment verification purposes and is limited to an individual's last position title, last location, and dates of employment. This holds true for former employees as well.

In 1976, IBM's privacy program was applied worldwide in the 124 countries where it does business.

Finally in 1981, IBM published 7 principles in handling personal data which took the issue of privacy beyond our employees.

1. PURPOSE OF FILE CLEARLY DEFINED and in support of valid company business.

2. COLLECTION ONLY OF PERSONAL DATA needed and, by fair, lawful means and reliable services.

3. USE LIMITED to defined purposes.

4. INFORMATION RELEVANT, correct, complete and up-to-date.

5. RIGHT OF ACCESS of data subject compatible with valid business interests of company.

6. SECURITY MEASURES adequate and relevant to classification of data.

7. PERSON RESPONSIBLE for file identified.

These principles or guidelines were applicable to both manual and computerized files and to all data subjects including both individuals and companies.

These self-imposed guidelines are in accord with the OECD "Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data".

We believe they provide maximum flexibility to meet changing technology yet provide the required protection of personal information. Hence our support at IBM for the OECD Guidelines which we hope Canada will support in the near future.

This brings me back to the question on the difference between the response of the private and public sectors to the issue of privacy.

In the case of the private sector, the relationship is selective. In other words, you can refuse to provide personal information if you feel the enterprise is not self regulating with regard to the way it handles its records.

On the other hand, there is a forced relationship with the public sector - that is, you are required by law to provide information from womb to tomb, for example birth and death certificates.

This is at the crux of the public debate on privacy and freedom of information.

I'm sure you will agree that you cannot approach this issue of privacy in the private and public sector in the same way. From all this I draw the following conclusions for the private sector:

1. Protection of privacy is a social responsibility shared by all users of personal information. Computers have not altered this.
2. Voluntary or self-imposed guidelines for access to personnel records are far better than legislated mandatory standards.
3. Governments must identify the basic objectives of privacy protection in all forms and promote their pursuit.

Initiatives on privacy can be likened to the introduction of the automobile - governments of the day considered a proposal that a person be required to walk in front of the auto with a red flag. Fortunately, responsibility for the operation of the auto was awarded to the driver.

ERIC WIMBERLEY *
Vice-President, Association Affairs
Canadian Cable Television Association, Ottawa

Good afternoon ladies and gentlemen. My name is Eric Wimberley and I am Vice-President, Association Affairs, for the Canadian Cable Television Association.

Our Association was formed back in 1957 by a group of entrepreneurial cable operators who recognized the need even at that early stage for some sort of coordination in the development of an industry which at that time represented only small pockets of the population mainly in the urban areas of Canada. Today the cable industry has grown to cover more than 60% of the Canadian population. The CCTA now represents some 380 cable licensees from Newfoundland to Vancouver Island who in turn serve some 4.8 million subscribers or approximately 95% of all Canadians who receive television via cable.

Background

Using a sophisticated antenna system, the cable operator is able to offer his subscribers signals which would not otherwise be available to them. Until a few years ago a typical system however still consisted of the basic twelve channels located in the VHF band. Today, 35 channel systems are considered more or less normal in Canada, and 54 channel systems are not far away. In the United States, where the regulatory environment is considerably different to Canada, 108 channel systems exist.

The variety of services which can now be offered to a subscriber by the television system is one reason we are here today. Until very recently every cable subscriber to the system received the same signals. A cable was installed from the trunk line on the street to the subscriber's TV set and the complete range of signals offered by that particular cable company was brought into the home.

Discretionary Services

However, with the advent of Pay TV just over a year ago, cable operators were able to offer their subscribers a number of discretionary services, discretionary in that the subscriber can choose to receive the additional service or not, or in fact to receive only a portion of the additional service.

This fact has led to the requirement for a device in the home which most people know as a decoder but which is more properly termed a home terminal unit. This unit enables the cable operator to address each individual subscriber to his system directly from the cable company office and to offer each individual subscriber the particular discretionary services which that subscriber wishes to receive. Obviously the cost of the service to a particular subscriber will depend to a degree upon the services to which he chooses to subscribe.

---

* Mr. Wimberley is the Vice-President, Association Affairs, for the Canadian Cable Television Association in Ottawa. He joined the cable television industry following a 15-year career at the senior management level with Computing Devices Canada Limited and Leigh Instruments Avionics Division.

In order to provide adequate service and to properly bill the customer, the cable operator must of necessity know just what services that subscriber is receiving. The simple recording of this information should not in itself be considered a threat to the subscriber's privacy. It is simply the recording of information necessary for billing purposes, similar to that recorded for example by the telephone companies in relation to long distance charges.

Sometime in the future however we expect to provide two-way services to our subscribers. The service will be provided and the individual subscriber's response to the service will be received in the cable company office. It is the collection of this individualized data which has led the cable industry to review its position as to its responsibilities regarding treatment of that data and what effect this information might have on the privacy rights of a particular subscriber.

Although a very few cable systems are experimenting with two-way services even now, in our opinion it will be some time before these services become widespread. Fortunately this provides time for us to assess the situation and to develop a workable code which addresses the interests of both the consumer and the industry.

The Study

Early in 1983, immediately following the introduction of the first discretionary services, the cable industry, through its National Association the CCTA, initiated a study into the necessity for a Code of Privacy for the industry. We looked first to our counterparts in the United States where discretionary services have been in existence for some years.

We reviewed the existing codes of a number of large cable companies and American Associations including Cox Cable of Atlanta, Georgia, the New Jersey Cable Television Association, the New England Cable Television Association, the Videotex Industry Association of Washington, D.C. and the often mentioned Warner Amex Code of Privacy. In addition, the Privacy Code developed internally by Rogers Cable, the largest cable operator in Canada was also examined.

Through this study, we have developed what we believe is a Privacy Code which will adequately protect the interests of cable subscribers in Canada. Earlier this year it was reviewed by our Board of Directors and it in turn has recommended acceptance by the National Association membership. The proposed Code will be discussed at the Annual General Meeting scheduled for the second week of June in Ottawa at which time we expect it will be accepted by the general membership of the Association.

The Code

While I obviously am not at liberty to release the proposed Code pending acceptance by the membership I can outline the areas of concern which it addresses.

Information Collection: The Code will require that individual subscribers be made aware of the information which is being collected and the reasons for the collection of that information. Only information necessary to permit billing or to provide adequate service to the subscriber will be collected and will be retained only as long as is necessary for billing or servicing purposes and will then be destroyed.

Security: All reasonable steps will be taken to ensure the physical security of the information collected. Access to data collected will be restricted to employees who are directly concerned with the operation of the services involved.

Subscriber Access: Subscribers will be allowed reasonable access to information on file and the right to have erroneous information corrected.

Third Party: Adherence to the Privacy Policy will be required of any third parties who may participate in providing services to the cable companies' subscribers.

Legal Compliance: Individual subscriber information will be made available to government agencies only under court order or other legal compulsion and, unless prohibited by law, subscribers will be made aware of any such legal requests for information.

Policy Review: And finally since our industry is subject to very rapid change, there must be provision for a review of the Code of Privacy, in order to ensure that current legal and technological developments are adequately addressed.

Industry Position

We believe a voluntary code will adequately address privacy requirements of the cable industry and will provide the flexibility which is necessary for the cable industry to adapt to the rapidly changing environment in which it must operate.

While cable is viewed in many quarters as a monopoly, and perhaps at one time this was true, such is not the case today. Today cable must compete with a variety of other services all trying for the subscriber's time and dollar including live theatre, more sophisticated home antennas, earth stations which can receive a wide variety of satellite delivered services and of course the recent explosion in the home VCR market.

Government regulation is not new to our industry. The Canadian Radio-Television and Telecommunications Commission closely regulates what a cable system can and cannot do. However even this Commission has recognized the need to ease the regulatory load wherever possible in order to allow the cable industry to respond adequately to the increasingly competitive environment in which it finds itself. In our view, government regulation, either federal or provincial, of a matter which can adequately be addressed by the private sector would be premature.

Of course there is another way. One well-known writer stated that "in order to avoid invasion of privacy, one need only arrange one's affairs in such a boring fashion that no one wishes to find out about you in any case".

Thank you!

PANEL 4: PUBLIC SECTOR PANEL: "PRIVACY: SOME PRACTICAL SOLUTIONS"

CHAIRMAN: Jacques Fremont *

PANELISTS: Hugh V. O'Neill

Caroline Pestieau

Douglas D. Smith

COMMENTATOR: William Atkinson **

---

* Professor Fremont, a member of the Quebec Bar since 1978, is currently Assistant Professor in Public Law at the University of Montreal Law School. From 1978 to 1980 he worked on a Ph.D. thesis at the London School of Economics and Political Science on the Judicial Control of Confidential Administrative Documents in a Comparative Perspective. His thesis is currently being completed.

* Mr. Atkinson is a barrister and solicitor who worked with the Quebec Government from 1975 to 1983. He was involved with the drafting of Bill 65 in Quebec, an Act respecting access to documents held by public bodies and the Protection of Personal Information. Mr. Atkinson is currently in private practice with Drouin and Associates in Quebec City.

ABSTRACT: FAIR INFORMATION PRACTICE AND COMPUTERS

HUGH V. O'NEILL *
President
American Society of Access Professionals

Background of Fair Information Practice

More than a decade ago, an advisory committee to the U.S. Department of Health, Education and Welfare issued a fundamental statement of information policy and practice in a report called "Records Computers and the Rights of Citizens".

The July 1973 report of the Advisory Committee on Automated Personal Data Systems found that, at that time, a person's privacy was poorly protected against arbitrary or abusive record-keeping practices. To safeguard the privacy of individuals and in recognition of the need to establish standards of record-keeping practices appropriate to the computer age, the report recommended the enactment, by Congress, of a Federal "Code of Fair Information Practice" for all automated personal data systems.

The five basic principles on which the Code rests are as follows:

1. There must be no personal data record-keeping systems whose very existence is secret.

2. There must be a way for an individual to find out what information about him /her is in a record and how it is used.

3. There must be a way for an individual to prevent information about him/her that was obtained for one purpose from being used or made available for other purposes without his/her consent.

4. There must be a way for an individual to correct or amend a record of identifiable information about him/her.

5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

There are certain exceptions to these principles in the interest of some greater need -- a couple of examples:

1. There are times when individuals should not be given access to records on themselves, e.g., in order to protect confidential sources in investigations or in the interest of national security.

2. There are times when other societal goals outweigh the need for privacy, and that in such cases information should be disclosed and used without

---

* Mr. O'Neill has been the Privacy Act and Fair Information Practices Officer for the Department of Health and Human Services, in Washington, D.C., since the U.S. Privacy Act became effective in 1975. He represented the Department on special task groups set up by the President's Domestic Policy staff to review the recommendations of the Privacy Protection Study Commission and worked with the President's Privacy Initiative staff and components of the Department on the development of new privacy legislation. He is also President of the American Society of Access Professionals.

the consent of the individual for purposes other than the specific purpose for which the information was originally collected, e.g., in compelling circumstances affecting the health or safety of a human being, including life-threatening situations.

A balance must be struck so that all statutes, regulations, and policies controlling personal information incorporate the basic principles of the canon while at the same time permit society's other goals to be effectively and efficiently achieved.

Both sets of goals may be achieved by adhering to the principle of due process, including openness in the decision-making process. Exceptions to the Code's principles should be permitted only when the public at large has been alerted, through congressional or state legislative hearings, notices of proposed rulemakings, open deliberative meetings and through professional literature and the general media. It is essential that interested parties, including the public whenever appropriate, be given an opportunity to participate fully in the decision-making process, e.g., the decision to use/disclose information for purposes other than those for which the information was originally collected.

Decisions to make exceptions to the privacy rights guaranteed individuals by the Code's principles should only be made at the highest and most responsible level of government and should take the form of a Federal or State statute, presidential executive order, order of the governor, or formal rule or regulation, so that the public will be fully informed of any action taken.

The Privacy Act of 1974 was the first legislative step in implementing these principles on the Federal level. At the State level, ten States have thus far enacted a comprehensive privacy protection law--either called a Privacy Act or a Fair Information Practice Act. The ten States are: Arkansas, California, Connecticut, Indiana, Massachusetts, Minnesota, New York, Ohio, Utah, and Virginia.

Computer Technology - 1984 and Beyond

The following characteristics are relevant:

- Increased speed--moving toward a billion operations per second and larger memory capacity
- Fifth generation of computers to include artificial intelligence
- Computer networks--central computers with terminals
- Network of Computers--large central processing systems connected
- Network of data banks devoted to a single area of interest
- Network of data banks devoted to a variety of interests
- Personal computers, home computers, word processors operating in both networks and as stand alone machines
- Both technical and management problems with respect to computer security--computer crime on the increase
- Computer-matching used to compare records on millions of individuals in different data banks--operating at various levels of government: Federal, State and Local
- The connection of government and private sector computerized data banks
- International computer networks cross the boundaries of national law.

Conclusion

Considerable effort has been expended to attempt to maintain adequate and reasonable safeguards for the use of computerized information systems. The legislative and executive branches have both tried to implement the fair information practice principles. However, there is a need for a continuing and even an increased level of effort, if we are to

use the most advanced computer -communications technology and still protect the rights of individuals.

Recommendations

The following initiatives for 1984 and beyond:

- Enacting Federal legislation and designing model state statutes for computer protection/crime situations
- The use of computer technology for the implementation of fair information practice principles, example: access to an index of personal data files through remote user terminals, computer techniques to enhance security
- The design of safeguards for computer applications especially for computer-matching and screening--general safeguards in legislation, more detailed safeguards in regulations and policy statements
- Follow-up, audit, evaluation to ensure that practice follows the legislative, regulatory and policy safeguards
- The drafting of second generation fair information practice statutes (The Privacy Act of 1974 is an example of a first generation fair information practice statute)
- The establishment of an entity with adequate resources and priority to:
  - assist in the above recommendations
  - to perform long-range planning - trying to lock the barn door before the horse is stolen
  - assist in the controlled sharing of computerized information

In sum, both the entity in the executive branch and the legislative branch should work toward the implementation of a proper balance so that statutes, regulations, and policies controlling personal information incorporate the basic principles of fair information practice while at the same time permit society's other goals to be effectively and efficiently achieved.

CAROLINE PESTIEAU *
Commissioner
Quebec Access to Information Commission

In the next few minutes, I will be discussing the main data protection features of Quebec's Freedom of Information and Protection of Privacy Law. Before I begin, I should like to explain my understanding of the "practical solutions" in the title of our panel today.

More than two dozen countries, states and provinces have adopted Data Protection laws. In each case, their lawmakers have had to choose from a menu of principles, institutional arrangements, procedures and definitions.

In this presentation, I will be looking at the strategic choices Quebec's National Assembly made when it adopted an Act respecting Access to documents held by public bodies and the Protection of personal information in June, 1982. I will devote most of my time to highlighting the essential characteristics of our law in the Data Protection field, after which I will mention one or two of the strategic options facing the body responsible for supervising the implementation of the act, the Quebec Access to Information Commission, of which I am privileged to be a member.

There therefore won't be much in the way of nuts and bolts of individual cases in this talk. However, on July 1st, when the main provisions of our law come into force, we will deal with the individual problems and cases which arise according to the principles and procedures established by the law. In this sense, my presentation is practical. I am talking about rights and obligations embodied, since June, 1982, in legal and institutional machinery. Since Quebec is so far the only Canadian province to have full-fledged data protection legislation, I believe that this exercise may be worthwhile to others who are considering what type of machinery to adopt.

The Access Law

I will be referring to the Quebec law by its short title as the Access Law. Despite this somewhat confusing nomenclature, the part of the law which concerns us today is essentially a Fair Information Practices Act. It shares a number of features with all such acts. First of all, it states that nominative, that is personal, information is confidential unless the person the information concerns authorizes its disclosure.

As corollaries to this principle the Access Law requires that only necessary personal information be collected, that the agency representative who collects the information inform the person concerned or data subject of the purpose for which it is being collected and to

---

* Mrs. Pestieau was appointed in December, 1982 as a Commissioner on the Commission of Access to Information, Quebec. She is responsible for the Commission's Montreal Office. As a member of the Pare Commission into Citizen Access to Government Information and Protection of Personal Data, which submitted its report Information and Liberty in May, 1981, Mrs. Pestieau was already familiar with many of the issues which the Commission will be addressing.

She was educated at Oxford University (M.A. Modern History), L'University Catholoique de Louvain (B.A. Philosophy) and McGill University (M.A., Economics).

whom it will be released. The collecting or holding agency is responsible for the accuracy of the information it holds and for its destruction when it is no longer needed. The data subject has free access to his/her personal data file. He/she can request corrections if the information on file is inaccurate, incomplete or equivocal or if the collection was illegal. In all such instances the burden of proof rests with the agency.

What is special about Quebec's Data Protection Law? In opting for certain mechanisms, principles and procedures, rather than for others, the Quebec lawmakers moulded the law in a particular way. I should like to review five of its principal characteristics with you: the legal context, the law's coverage, its attitude to Government as a repository of personal data, its creation of a supervisory commission and its detailed nature.

The legal context

The Quebec law guarantees both freedom of information and data protection in one act. Freedom of information and privacy are the subjects of chapters II and III respectively, while the general provisions of the other chapters apply to both these rights. All three Commissioners are responsible collectively and individually for both sets of rights, although, as we shall see later, the Commission's mandate is wider in the case of data protection than in the case of access to administrative documents. There should therefore be no downgrading of one set of rights with respect to the other.

The Access Law is a fundamental law which takes precedence over all subsequent legislation unless a new law expressly states that it applies notwithstanding the Access Law. One of the Commission's tasks is to examine existing legislative provisions which are inconsistent with the Access Law and recommend amendments in one law or in the other. In the absence of harmonizing amendments, inconsistent provisions are automatically suspended three years after proclamation of the Access Law, that is to say, in October, 1986.

The Access Law also has its own sunset clause. Five years after its proclamation, the Quebec Access to Information Commission has to report to the Government on the way in which it has been working and on the advisibility of maintaining or amending it. The Government tables this report in the National Assembly which decides on the law's future within the following year.

Coverage

The Quebec Law only applies to the public sector but it gives that sector a very wide extension. Whereas the federal law applies to about 130 agencies, the Access Law covers about 3,600, including towns and cities, school boards, hospitals, universities and crown corporations.

These agencies cannot ignore the law since in each the person exercising the highest authority automatically becomes the access and privacy coordinator unless he/she delegates this responsibility to another management person. Although the law does not cover the private sector, it does regulate the flow of personal data between public and private agencies. For the sake of completeness, I should also mention that the Access Law applies to both manual and automatically processed files.

A particular characteristic of the Quebec Access Law is its coverage of so called "confidential" files. The Government can authorize the setting up (or the continuation) of a confidential file by an order-in-council specifying the kind of information to be filed, the use to which it is to be put, security and conservation measures to be taken and the categories of people having access to it. Before making or amending such an order, the Government has to obtain the opinion of the Commission and the order itself and the opinion are tabled in the National Assembly.

Naturally, the people concerned do not have access to their records in confidential files, but the Commissioners do. They can investigate a confidential file to determine whether or not the personal information it contains was entered and used in accordance with the order tabled by the Government.

Government as a repository of personal information

Under this heading, I should like to say a few words about the way in which the Access Law considers public bodies as recipients and repositories of citizens' personal data. It is clear from the law that a citizen who provides information to a public agency, usually as a condition for receiving a service, does not yield it up to a monolithic Administration which can use it in whichever branch of its activities it pleases.

Data is collected by one of the three thousand six hundred departments, hospitals, crown corporations or other bodies not by the Government of Quebec. Thus data collected by a particular hospital is not necessarily available to the Department of Health, data on eligibility for welfare is not automatically available to educational officials screening bursary applications and so on. One agency can only release data to another under a written agreement tabled in the National Assembly to which the Commission's evaluation of the proposed transfer is annexed.

Thus everyone can find out to whom the agency which originally collected his/her data may be releasing it.

The Access to Information Commission

I now come to the fourth and one of the most important characteristics of the Quebec Access Law - its creation of a special agency to supervise implementation of the law. In contrast to the situation in the United States where citizens themselves have to take legal action if their freedom of information and protection of privacy rights are not respected, Quebec has set up a three-member commission to make sure that the new rights it has accorded are respected.

The Commission is a hybrid body with tasks akin to those of an administrative tribunal, a regulatory agency and an advisory body. Acting as a tribunal, its first duty is to hear requests for review of administrative decisions regarding access to public documents and access to personal data files, as well as requests for the correction of such files by the persons they concern.

The Commission's decisions on questions of fact within its competence are final and it can issue a binding order: "to release a document or part of a document, refrain from doing so, correct, complete, clarify, update or delete any nominative information, or discontinue the use or the release of nominative information".

While its duties on the freedom of information side are essentially limited to reviewing agency decisions, the Commission also acts as a supervising body in dealing with personal data. Agencies have to declare all their data files to the Commission which draws up the declaration form. The Commission draws on these declarations to publish and update an index of all personal information files maintained by public sector agencies. It is responsible for authorizing the release of personal data for research purposes and has various other administrative functions.

The Commission's third major task is to give the Government its opinion on a number of questions, the most important of which have already been mentioned - data linkage agreements for the transfer of personal information between agencies and the creation or modification of confidential files. With respect to the former, it is worth mentioning that the Access Law does not set out principles to guide inter-agency data exchanges, such as routine or compatible use, so the Commission has had to develop its own thinking in offering advice on proposed inter-agency data releases.

The members of the Commission are appointed by the National Assembly for a five-year term of office and can only be dismissed by a two-thirds majority of the Assembly. Their annual reports, and any special reports they feel the need to present on non-compliance with the act, are examined by the Assembly within a statutory time period. The Commission's independence vis-a-vis the ad-

ministration in general is thus based on its relationship with the Legislature. The law does allow the Government to use an executive veto against an access decision of the Commission, in which case the Commission will have to rely on the credibility it has established with the media and public opinion to maintain its independence. This veto, however, mainly applies to the freedom of information part of the law. Apart from a possible application to a data subject's access to his/her file, the Commission's powers in the data protection area are unaffected by this form of executive control.

The Access Law's precision

The last characteristic I want to discuss with you is a qualitative one that I have not been able to put a name to. It concerns the degree of elaboration in the Access Law.

Quebec lawmakers obviously wanted to avoid problems which had arisen in other countries as a result of administrative inertia or of imprecise drafting. As a result they included a number of detailed requirements some of which go further than those in most other data protection legislation.

One example is an agency's obligation to record each non-routine consultation of a personal record file and to make this record available to the data subject. This in turn leads to a definition of types of employees who may consult the file on a routine as opposed to a non-routine basis. In their determination to avoid the ambiguities which have cropped up elsewhere, the authors tried to plug all the loopholes and as a result have produced an elaborate set of rights and obligations.

On the one hand this makes the work of the Commission easier. Many of the problems which would have inevitably surfaced sooner or later are already identified and can be worked on. On the other hand, there is a danger of the Access Law giving rise to an arcane bureaucratic set of procedures which lose contact with the fundamentals of data protection. The members of the Commission are well aware of this danger and intend to avoid getting bogged down in bureaucratic hassles while using the detailed provisions of the law to their best advantage.

Strategic choices facing the Commission

I have just mentioned one important choice in referring to the Commission's determination to prevent the freedom of information and data protection procedures from becoming overly bureaucratized.

I would like to conclude by raising two other questions which are among the many that the Commission will have to address as it carries out its mandate.

The first concerns the right balance between concentrating on responding to individual citizens' requests regarding their own personal files - access, correction, conservation, etc. - and allocating resources to auditing agency files in order to insure compliance with the law.

The two activities are obviously closely interconnected. Individual requests may signal the need for an audit, while an efficient audit will act as a preventive measure eliminating abuses about which citizens might have complained. While there is no question whatsoever of downgrading citizens' requests, experience elsewhere has shown that these are often insufficient to insure agency compliance which requires, in addition, active encouragement and monitoring.

A second strategic option is that of the Commission's stance vis-a-vis agency file holders. When not acting as an administrative tribunal, the Commission could choose to work with the file holders in the agencies in developing acceptable standards for collecting and managing personal information as the German Federal Commission appears to have done. Or it could keep its distance in policing personal data processing according to the principles of the law.

Obviously there can be no hard and fast, a priori, answers to either of these questions. I have mentioned them in order to share with you some of the challenges a law such as the Access Law, which creates new rights, obligations and institutions, inevitably sets for those who have to oversee it implementation.

The Access to Information Commission is at the moment a hive of reflection and activity in preparation for the proclamation of the main articles of the law on July 1st. In the course of responding to the diverse situations which will arise, we hope to make the choices most appropriate to the law's objectives which are to insure freedom of information and protection of personal data without depriving Quebecers of a responsible and efficient administration.

DOUGLAS D. SMITH *
Assistant Deputy Minister
Communications Policy Branch, Department of Justice
Province of Saskatchewan

Privacy is not the issue that we are dealing with here at this Conference. The electronic age has taken us far beyond the point of the old notions of privacy. People today have to adopt new attitudes towards this subject; we have to think in terms of new forms of privacy.

It is a given that files are held on us; on any one of us who has ever applied for a mortgage, for a Visa card, visited a doctor, opened a bank account, or applied for any one of a thousand credit cards that are available. For the convenience of getting access to credit, we have wittingly - or unwittingly - forfeited our privacy.

For the speed and the convenience of pulling money out of walls when banks are closed, we have made ourselves naked. There are those among us - the civil libertarians - who would have us return to the dark ages, who would have us believe that it is wrong that people can collect information on us. But you know, absolute privacy is a fairly modern notion. It did not exist in the Greek City State, and it did not, and still does not, exist in communities of 500. Information about people living in small communities is very public.

However, what disturbs people today is the enormous amounts of information that can be stored about them, the kinds of information, the possible mis-use of that information.

And this is what this Conference is all about. Not privacy, but the mis-use of information. This is the real issue. I personally do not mind people collecting information on me, but I ask them not to use it against me maliciously. The question we should seek answers to is: "Are there ways of controlling the mis-use of this information? How can we make the collectors of information accountable?"

And, the issue is not new. Shakespeare in Othello said:

> "Who steals my purse, steals trash; tis something, nothing; t'was mine, tis his, and has been slave to thousands; but he that filches from me my good name, robs me of that which not enriches him, and makes me poor indeed".

Now then, I am sure they did not have computers in Shakespeare's time, but he too was seized with this problem as we are in Saskatchewan. My Minister, The Honourable J. Gary Lane, is responsible for the publicly-owned telephone company, and is responsible for SaskComp, the largest computer installation in our Province.

---

* Mr. Smith, currently Assistant Deputy Minister, Communications Policy Branch, Saskatchewan Department of Justice, has held positions such as: Associate Deputy Minister with Manitoba Government Telephones; Associate Deputy Minister of Communications and Information Services for the Government of Manitoba; Manager of Francis Williams and Johnson, Communications Consultants, Calgary and Edmonton; and Vice-President, Western Canada, McConnell, Stevenson and Kellog, Communications Consultants, Western Canada Head Office, Winnipeg.

My Minister, my Government, has a very real interest in ensuring that the telephone company system is not mis-used by those who would transport information across the system. But, at the same time, this concern is tempered by the knowledge that too strict legislation or severe conditions on users could stifle initiative to introduce the myriad of new telecommunications services now here and on the horizon.

We have, as many of you may know, the longest fibre optic system in use anywhere in the world in Saskatchewan. It has tremendous capacity, and tremendous capability for two-day interactive data. We have also in the past couple of years been gaining invaluable experience from information systems such as the Pathfinder Trial, and the Agritex service now in use.

The experience gained from the Pathfinder project has assisted information vendors and SaskTel in developing a more sophisticated videotex arrangement. This will allow subscribers who have the appropriate equipment to access information from one of several potential data bases that are located in remote and independent locations. This is possible because SaskTel now owns and operates a gateway computer that both facilitates uniting users to the data base they require and accommodates the necessary billing process. The gateway service which SaskTel offers is the first such commercial gateway of its kind in North America. The service is called Agritex and the data bases that are available through it are available through one of the two protocols.

What are the implications of these technologies and services to the public? The first important implication is that our telecommunications services allow business people and residents of Saskatchewan to conduct their business internationally, nationally and locally from their place of business or home. International markets and contacts can be accessed easily and large quantities of information can be exchanged efficiently.

Second, the new technologies create a vista of new economic opportunities. The information industry that I alluded to earlier is one that is being encouraged by the Government of Saskatchewan. It offers opportunities in both software - the knowledge and information necessary to operate or use the new technologies - and hardware, the equipment itself. Advancements in technology, however, frequently are accompanied by social concerns. The technologies that allow us to process and exchange information over great distances bring with them concerns for individuals and our right to control information about ourselves.

You will appreciate from earlier remarks about advances that have been made in communications technologies in Saskatchewan, that the issue of personal information brought about by the new technologies is a reality not a hypothetical situation. Accordingly, the Government of Saskatchewan appreciates that this is an important issue and one that requires effective attention. This appreciation is reinforced in the Province because SaskTel, the Province's Telco, is, as I already mentioned, owned and regulated by the Province.

This means that Government can ill afford to have advertisers or information vendors compromise the public. It would seem, therefore, that protection of an individual's rights will require some form of public sector intervention by governments.

The concern over the issue of information is more widespread than I have suggested to this point. The Europeans have recognized, acknowledged and taken measures to protect all individuals' rights. The Council of Europe and the EEC have co-operated to develop a set of principles that are intended to guide countries in the preparation of legislation. A European Convention respecting privacy has been passed: participating countries ratified the Convention by passing legislation.

Great Britain is one country that is in the process of passing privacy legislation. This legislation, which we will be hearing more about tomorrow from the Honourable David Waddington, Minister of State for the Home Office:

-"...will establish a Data Protection registrar, who will maintain a register of personal data users and computer bureaux and powers to ensure that data are used in accordance with (certain) general principles...;

-sets up an Appeal Network for data users; and

-gives data subjects certain legal rights, including a right of access to their personal data and in certain circumstances a right to compensation."

It would seem that the onus for intervention by government is strongly emphasized when environmental concerns and issues like privacy become too large for the individual to control himself. But is there another side to issues of this nature that needs to be taken into consideration to balance public sector intervention?

Consider, for example, benefits that are derived from advances in computing and communications technologies. Consider also, the vendors of these services. Public sector intervention should not deprive society of benefits nor smother enterprise but instead should seek to create a climate and framework to foster the good and obliterate the evil. Can legislation, such as that which the British Government is introducing, achieve this?

Private sector interests that are represented by organizations like the CCTA or fledgling information companies can be anticipated to argue that legislation or regulation will impair their ability to provide the type of service the public wishes at a reasonable price. Public sector intervention, particularly legislation, frequently is perceived by such organizations to be burdensome, expensive and a threat to the information industry. This, however, need not be the case. Legislation can assist both the public and information vendors. How can this be, particularly with an industry such as the information industry that employs such novel technologies like videotex?

The proposed British legislation which I cited a few moments ago and which we will be hearing more about tomorrow, has the potential to protect the public interest and to help foster an information industry. The registry concept and associated regulations on which it is based, facilitiates the public interest by establishing the rules of the game and the sanctions for non-compliance.

Information companies operating within the framework of the legislation effectively will be accommodating privacy concerns as defined by publicly responsible legislators. The public, consequently, will perceive these companies to be law abiding and thus worthy of its trust. This perception is important to information vendors because it is unlikely that the public would patronize them if their integrity was suspect. Thus, legislation would afford a certain status to information vendors, and this status would have value in both moral and commercial terms.

Commercial interests could be further served by legislation that employs the registry concept. The agency of government that registers and polices information vendors could make the list of registered vendors available to patrons. Public attention thus would be directed to those companies that are known to government and who are subject to government sanctions if they do not conform to the legislation that protects the public interest. This too has commercial value and can help to foster the industry by ensuring that companies operating in it are honourable.

I believe that legislation which embraces the registry concept is worthy of our consideration and attention. Worthiness is an important concept to Saskatchewan legislators because government policy in Saskatchewan is directed toward reducing or precluding regulations or legislation that are not necessary. I believe that the case for legislation as it pertains to personal information is strong: I reiterate that the registry concept in legislation should be considered. But, how can this come about in a country with two senior levels of government and several jurisdictions?

The Europeans again have provided a model that we could follow in preparing such legislation. Earlier in my remarks, I alluded to the concept they have employed. This involved the relevant countries, or jurisdictions in our case, developing and agreeing to a set of principles that would establish the framework for legislation in each jurisdiction. Communications between those individuals charged with the responsibility for creating legislation in their respective countries helped to ensure compatibility and acceptability among countries that agreed to the set of principles.

This method of proceeding could accommodate the types of concerns that are evident in the respective levels and jurisdictions of government in Canada; each jurisdiction could have its unique circumstances accommodated without threatening the general intent of the agreed principles.

We in Canada are fortunate with respect to this issue in that a great deal of valuable work, principles, legislation and experience could be drawn from the Europeans. Furthermore, Canada itself has done a reasonable amount of work through the OECD. She has consulted with the provinces about the OECD guidelines and currently is deciding whether or not to adhere to them.

Clearly, the time of decision with respect to this issue is at hand. We have this excellent forum graciously organized by the Government of Ontario. I believe that we should avail ourselves of this opportunity to follow the European models, to use Canada's experience and to create a legislative mosaic to ensure that an individual's right is ensured at local, national and international levels. To this end, I would suggest that the levels of government and jurisdictions that are represented here establish a committee, the members of which would be charged with two responsibilities: (1) creation of a set of principles to guide the development of legislation in the respective jurisdictions, for which we have valuable information to help that process along, and (2) once the principles have been agreed to, co-ordinate the development of legislation in the respective jurisdictions. I believe that legislation of the type I have described today will protect the public interest, help to foster the information industry and assist in improving international relations through a medium that can assist both social and economic well being.

Thank you.

PANEL 5: "PRIVACY: INITIATIVES FOR THE PRIVATE SECTOR"

CHAIRMAN: Ed. Finn *

PANELISTS: W.H. Loewen

Boris Mather

Maryon Brechin

---

* Mr. Finn, a journalist for fifteen years and formerly public relations consultant to the Canadian Labour Congress and Public Relations Director at the Canadian Brotherhood of Railway, Transport and General Workers, is presently employed as a Senior Public Relations Officer to the Canadian Union of Public Employees.

W. H. LOEWEN *
President
Canadian Independent Computer Services Association
(C.I.C.S.)

It is difficult as a data processor to suggest specific initiatives in the area of privacy. I could come forth with a series of platitudes about how we should be self-regulating, how we should act responsibly or even explain the technology that we should be applying to help ensure privacy.

I don't believe any such statements will ever satisfy the public. I am even more certain that they will not serve the long term needs of the computer services industry.

The two major issues to be dealt with are access to data by the proper persons and no other, and secondly, the misuse of data by the party in possession of it.

I personally do not believe we can rely on self-regulation in either case.

- There will always be those who will abuse the regulations and their conduct will reflect on all businesses -- the responsible as well as the irresponsible.

- The cynical public will not be left comfortable in a self-regulated atmosphere. There may well be an attitude that the codes adopted are merely window dressing. Again, that attitude will apply to all data collectors.

- Self-regulation favours the least scrupulous operators because they may be able to put themselves in a position of competitive advantage by misusing or selling private information.

- Industry codes do not have the force of law and breaking them does not reflect on the individual company in the way that legal action would.

This is a legal problem that must be solved by the legal profession and our legislators. Persons holding private information should be viewed as holding that information in trust for the purpose for which it is provided and for no other purpose. Anyone who violates that trust should be subject to severe penalty. The full force of the justice system should be placed behind the enforcement of those penalties. No initiative on the part of the industry can fill that void. The public must understand that they are protected by the law.

There is a substantial part of the public that believes that what is not illegal is legal. Most of the hackers who try to break into systems will surely stop or be stopped by their elders when it is clear to all that misuse of data is an offense. The public will accept the storage of their information if they know that abusers, corporate or individual, can be prosecuted.

---

* Mr. Loewen is President and Founder of Comcheq Services Limited, a company formed to provide computerized payroll services for companies. He is a Chartered Accountant who has spent most of his career in industry in positions of Financial Management. He has been active in the computer services industry as a founding member of Canadian Independent Computer Services Association (C.I.C.S.) and is its current President (1983-84). He is also very active in his community and is a member of the Sustaining Fund Committee on the Winnipeg Symphony Orchestra.

Determining how this can be done is beyond my competency. It is a problem for the lawyers.

What we in the computer services industry can do is warn legislators of problems that may be arising. This I will try to do now to the degree that I am able.

The potential for massive abuse is growing. The sequence of events and possible events relating to privacy in the area of banking provide examples.

Two or three years ago, the Royal Bank was caught searching its branches to find out where newly elected Member of Parliament, Cyril Keeper, did his banking. There was some indication that this was done with other MP's. The situation suggested that there might be a central depository of this sort of information on all MP's. Possibly similar searches could be made for other individuals. This was a clumsy effort. The Chairman of the Royal Bank explained that the bank merely wanted to be able to contact the MP, not being satisfied apparently with the methods available to the rest of us. That was not the inference taken by others when this act came to light.

There is a kind of intimidation of everyone when powerful institutions use information for reasons not directly related to the purpose for which it was obtained. Had the bank been a little more up-to-date in its procedures, it could have provided the appropriate officials with computer routines to search their files for the names of individuals that interested them. That way, the chances of such efforts as the Royal Bank engaged in would be less likely to come to light. Technology now permits such activity. The law should prohibit it.

The problem with banks is about to be aggravated many times over. Credit and debit cards are about to go on-line -- possibly world-wide. It will be quite an easy matter to follow, in real time, the activities of any card user. The potential here for snooping into other people's private lives, habits and activities is quite significant.

Industrial espionage could take on new dimensions as sleuths watch the movement of their prey from bar to airline to hotel. As we head for the cash-less society, will the person paying cash be viewed with suspicion -- as someone not wishing to leave a record of his whereabouts?

Our Manitoba Premier and a number of aides recently made a trip to Europe. The trip was surrounded by sufficient secrecy to ensure that it would be well publicized. Possibly he will come back with an announcement of some sort. With credit card transactions being handled on-line, his activities and possibly even the purpose of the trip could be discovered. This could provide advance information that would be of value to someone. How will such snooping be stopped? Possibly the examination of such transactions should be subject to the same restrictions as wire tapping.

Keep Data in Canada

The issue of transborder data flow involves privacy. How do we protect Canadian data when it is stored outside Canada?

An attempt to overcome this and other objections to transborder data flow has been proposed by the Royal Bank. Their approach is to enter into a treaty with the U.S. and possibly other countries that would ensure Canadian rights to data stored in the U.S. and vice versa. It is the implementation of an idea being expounded by some that calls for the "right of presence" of multinationals in the countries of their choice.

This is a very dangerous step. It is a back-door approach to giving multinationals greater access to business opportunities than, in this case, Canadians themselves have. It is obvious to anyone, that in the fast emerging computer-communication industry, there will be ten times as many applications developed in the U.S. as in Canada. It is not in the least that we are incapable of developing these applications. There are simply ten times more people working on the application in the U.S. than in Canada. Free access to the Canadian market via the telephone system

means that U.S. suppliers of services can treat Canada like another state of the union. This applies equally to systems provided by computer service companies and in-house systems provided by head offices to their subsidiaries.

This process complicates many decisions in Canada. It certainly complicates the privacy issue. It involves our sovereignty. Most importantly, it involves not just computer related jobs but management, clerical and other business services functions that will be performed where the information resides. The number of jobs could well be over 500,000 before the end of this decade. Let me give you an example of the apparent job loss.

The three largest automobile companies employed about 90,000 Canadians last year. Their U.S. parents employed nearly twice as many people to handle that volume of sales. The reason is, we believe, that not just the R & D jobs which we have come to expect to be performed outside our borders, but many other management related jobs can now be performed outside our borders. I invite you to check the employment levels of many U.S. multinationals operating in Canada and you will see that this is a general situation.

The answer to the privacy, sovereignty and employment issue is not a treaty with the U.S. that would paper-over these problems. The answer is to be found in the report of the Clyne Commission to the Minister of Communications who was then the Hon. Jeanne Sauve. Their recommendation was that Canadian data should be processed in Canada.

In what may turn out to be the greatest betrayal of Canadian interests in history, the Department of Communications has, instead, allowed the installations of facility after facility that is put in place for one purpose only -- the conducting of Canadian business from outside Canada.

The computer services industry can and will fight for the processing of Canadian data in Canada. We need the support of all Canadians who are concerned about our privacy and the level of unemployment in Canada.

A final area for concern has to do with satellites as they begin to be used for data and communications. That data rains on all of us. Are there safeguards to ensure that it is not interpreted by the wrong party?

In conclusion let me say that we need legislation that will ensure that information we provide as individuals must only be used by that recipient for the purpose for which it was provided. Violators of that trust should be subject to the same penalties that any other breach of trust would attract. The potential penalties should be very severe because the potential abuses are great. I have no fear of such penalties. I don't think other responsible holders of private information would have any fear either. It does not detract from the establishment of standards if an industry chooses to do so.

This does not appear to me to be difficult law nor difficult to administer. By using the principles already well understood and supported by precidents, both industry and the public can enjoy the benefits of new technology without unnecessary concerns.

ABSTRACT: FREEDOM TO ACT: TRADE UNIONS' CONCERNS WITH PRIVACY OF THE CITIZEN

BORIS MATHER *
Chairman
Canadian Federation of Communications Workers

These remarks outline three principal areas where unions are particularly concerned about invasions of the privacy of their members. Such privacy violations are not only demeaning and dehumanizing; they inhibit members' ability to act as free citizens, freely expressing their opinions and freely exercising their right of assembly and action as unionists.

The first concern is that employers often have access to personal information which could be used against a member in his or her employment situation. This has happened with inadvertent complicity by government. For example, in the 1950's communications installers employed by Northern Electric had information given in federal government security clearance procedures used by company personnel officers.

A more recent example is the casual way in which the Evalulife questionnaire of Health and Welfare Canada was circulated at BC Telephone in 1983. The union objection was not only to the availability of the material to management but the very questions themselves. We object to a government file, of whatever department, having answers to questions such as "Has anyone in your family ever committed suicide?" and "When did you begin regular sexual relations?" We consider that whole scheme to be an outrageous invasion of privacy and have advised our members not to cooperate with it.

Our second concern is with government accumulation of personal data on citizens. Unions by their nature are anti-status-quo and outside the Establishment, in Canada and Poland, El Salvador and South Africa. Police surveillance is a problem for union activists everywhere. We always and everywhere oppose the extension of secret police powers. Therefore we oppose the current federal security agency bill.

Third, we oppose electronic and auditory surveillance of our members. This is standard practice in telephone companies but we have never accepted it and we are still striving to eliminate it.

These are the three primary privacy concerns of the members I represent - unauthorized use of personal information, state snooping, and surveillance. We intend to continue to struggle against such abuses of civil rights.

---

* Mr. Mather has been active in unions for many years. Prior to 1973 he was Canadian Director of the Communications Workers of America (AFL-CIO). He is currently Chairman of the Canadian Federation of Communications Workers, a 50,000 member Federation consisting of three Canadian Trade Unions: Canadian Office Employees Union, Communications Workers of Canada (CLC) and Telecommunications Workers Union (CLC).

MARYON BRECHIN *
Consumers' Association of Canada Ottawa

Thank you very much, Mr. Chairman. Good afternoon. It is a little daunting to be asked to talk on the subject of consumer initiatives in privacy on the afternoon of a day which has brought forward so many perspectives on privacy, most of them with some reference to computers or communications technology. Undoubtedly, everything I say will already have been said in some fashion by someone else. But hopefully, privacy as consumers see it, may present some unique facets since it's basically personal privacy which concerns them most.

If I might take a minute to explain C.A.C., (Consumers' Association of Canada for those of you who aren't yet members) it's Canada's only voluntary consumers' association. It was established in 1947 as an offshoot of the Wartime Prices and Trade Board and now, with 160,000 members, it has several roles. We publish two magazines monthly, the Canadian Consumer and le Consumer Canadienne and we operate the laboratory which tests consumer products reported in the magazine. Since 1973 we have represented consumers before regulatory tribunals through our regulated industries program but the Association's greatest strength still is in the thousands of volunteers who are organized locally, provincially and at the national level - volunteers who provide information and assistance to consumers and present consumers' views and their problems to industry and government.

Our association first became concerned with the invasion of privacy in the 1960s when a flood of unsolicited credit cards deluged our mailboxes. The theft of these and their unauthorized use rose very high on the list of problems brought to the attention of our volunteers. But unwise authorized use of the new plastic money made some consumers aware for the first time of the Credit Reporting Bureau, which they discovered could have a very great impact on their lives even without any knowledge of their existence. Information, and more dangerously, misinformation could be held about consumers and dispensed freely. So the issue of privacy began to come to the fore.

We were aided by the work of the Law Reform Commissions in several countries and the consumer movement began to learn what information about an individual might be held and how it could be used. We made the shocking discovery that, although as far back as 1980 when two Harvard graduates whose names are very familiar now - Warren and Brandius - began to argue strongly for what they called the right to be left alone, still , in the 1960s Canadian law offered no specific protection for this very precious concept. This is perhaps understandable in the light of the difficulty we have even today in defining privacy.

Although is is a jealously guarded concept, consumers have widely differing ideas of privacy and of the weighting

---

* Mrs. Brechin, apart from being a former President of the Consumers' Association of Canada, has a lifetime of dedication to consumer advocacy. She has been an active member of the CAC for over 30 years. In 1975 she was named a Member of the Order of Canada for her outstanding achievement in the area of consumer affairs. Currently, she is Vice-President of the Conservation Council of Ontario and Canadian representative for the International Organization of Consumer Unions on the Codex Alimentarius Committee of the Food and Agriculture Organization and the World Health Organization.

they accord its various aspects. Each one of us has a core of certain matters which we deem so intimately ours that we have a right to exclude others, if we desire to do so. The prime requirement is perhaps that we, ourselves, retain control over what information is available to whom, at what time and in what form. Scott Gardiner, in his examination of the subject, suggests that it is the loss of personal autonomy or control that is of greatest concern, and that we need to determine an acceptable balance point between total loss of autonomy and a world of full self-disclosure. Whatever degree of personal rights are found acceptable, they should be equitable for all members of society and they should be so well understood that no one feels threatened.

The threat to privacy which was posed by Credit Reporting Bureaus and credit cards was a very interesting project for our Association. Volunteers searched out the Credit Reporting Bureaus in their areas and attempted to obtain access to their credit files. Some of them were denied and some of them found they didn't have any - they happened to be married. Their credit reports were in their husbands' names. Their reports to the Association added to the pressure which was brought to bear on governments to enact legislation which would govern the types of information which could be held, for how long, the provisions for informing the consumer when a negative report had been given, and the opportunity to examine and correct if necessary the information held. This pressure resulted in the passage, in most provinces, of credit reporting legislation, with which we are all familiar, and which embodied some of all of these provisions.

Then came the computer with its attendant data banks and host of link technologies, all to them with the potential to increase exponentially the threat to our personal privacy. In a number of surveys on these new technologies conducted by C.A.C., privacy protection has consistently been rated in the top three of the concerns of consumers.

In 1973 an Association's resolution first requested legislation to protect the privacy of individuals. What is consumers' prime concern? Perhaps on the broadest basis it is with the security of the information held. As we have seen, the concept of privacy doesn't exist in English Common Law although confidentially does, as in contracts. Some provinces make the violation of privacy actionable, without proof of damage, but there is still no federal statute which defines theft of information as a crime, although our Association has for some years requested that the Criminal Code be amended for this purpose. At the federal level, wire tap legislation forbids the interception of voice or electronic massages without a judicial order and there are provisions regarding the release of data collected under the Income Tax and StatsCan Act, for two.

Is is a small wonder that consumers are nervous about the safety of information about them even now held in data banks, and this concern increases when they learn that many of these banks are outside Canada and are not even subject to our minimum laws on the subject. The security of data collected through the use of the new technology is virtually still unaddressed. Some provinces have data based leakage provisions but no redress is available for breach of duty in data bank disclosure. Nor is there any legislation to limit the length of time information can be held on a person.

C.A.C. has recently become aware that existing credit reporting legislation can be bypassed by consumers when a request for an American Express credit card was denied a young man. He found out, after a great deal of searching, that clients of credit reporting agencies can use their identification number in computers to call up the file. There would be no negative reports given, the whole file just spills out and the consumer is never notified, has no opportunity to correct an error. This appears to be a technology-developed loophole which requires repair.

Computer-based technology is providing more than loopholes. Electronic data processing and advanced telecommunications systems together have removed most of the physical impediments to information collection and dissemination. Their capacity to collect, to store and most importantly, to correlate information about consumers is awesome, and it's rapidly growing. There is no doubt that the ability to amass and correlate data represents power in the hands of those who hold it, and consumers are correct in regarding it as a very real threat to privacy and individual autonomy.

The security of financial information may be slightly better covered but there is still no legal or legislative definition of an individual's right to obtain access to personal information held by financial institutions in order to verify or correct it. In addition, consumers are now nervous about the changes which concentrate information about them in a central data bank instead of spread out in their local branch banks and credit unions. Banks tell us that they have safeguards but I don't think any one of us has not had to deal with computer breakdowns when we go to make a deposit or withdrawal and that scarcely leads us to have confidence in the system. And engineers tell us that there is no failsafe system. In the words of one, what the mind of man can devise, another can break.

Another facet that concerns us is that computer students often practice means of entry into data systems as part of their training. C.A.C has expressed its concern that the moral issues posed by this practice are inadequately dealt with by our colleges and universities.

The introduction of point of sale systems can also pose a threat for unauthorized access and use of information. C.A.C. volunteers have been working with P.A.C.E. (Payments Alternative Communication Exchange), and I think all of you heard about P.A.C.E. at the last session. We've been working on the development of what we hope might be a self-regulatory practice for such systems. The debit card which they will use will require much more sophisticated safeguards than credit cards which we now use since the computer can't match signatures. But we're concerned that industry seems to be dragging its feet a bit in the development of voice or thumbprint or some other method of identification. Perhaps, because as presently planned, debit cards shift the burden of unauthorized use to the consumer.

P.O.S systems will generate masses of information about our habits which have great value to industry and over which we have no control. Our only safety appears to lie in not using the system. The only answer may be legislation, for the compilation and analysis of this data can be far more injurious to consumers that the practices which have caused us so much concern in the past - the sale of subscriber lists to mailing industries (the junk mail syndrome), telephone solicitations and even now the telephone solicitations come by computer to consumers (we hear a computer voice on the phone asking us questions and asking for our support), and also the blacklists of names of people which have been prepared and sold to landlords, to insurers, and others.

Perhaps the most information-hungry invader of our privacy is government itself. We just have to look at the federal Statistics Act, for one, and I think some of us can still recall when the Prime Minister, Lester Pearson, was asked whether the S.I.N. number would ever be used for other than social assistance programs. And his answer, "certainly not", must be the most ironic assurance we've ever had in Canadian history because so widespread is the use of the S.I.N. number now that the C.A.C. in 1979 requested government to provide adequate safeguards for the protection of the privacy if individuals in any system using S.I.N. numbers and we also adopted an Association policy of alerting consumers to the dangers of the indiscriminate use of this number.

Unfortunately, not all consumers realize how prevalent is the collection of information today. Then Privacy Commissioner, Inger Hansen, found two

years ago in a study that many consumers do not even realize that they can refuse to divulge personal information. A much more focussed effort will be necessary to alert consumers to the need to give the bare minimum of information required. However, restriction of the use of personal information to the purpose for which it was collected may require legislation similar to that in effect in Sweden. This legislation would require zealous application and monitoring to be effective, perhaps through licensing requirements as are used in some European countries. This suggestion was made by the Association in a brief to the Committee on Computer Crime.

But what of redress for the injured consumer? Even if the Criminal Code is amended and the right to privacy enshrined in the Charter of Rights and Freedoms, as our Association has recommended, it will still be costly to bring a case before the courts. Under the Privacy Act the Commissioner can appeal for a citizen against the federal government and its agencies. Do we require provincial privacy ombudsmen to assist consumers against the omnipresent data banks in the private as well as the public sector? C.A.C. has also recommended periodic public reviews of computer security in both sectors, the development of standards for security, mechanisims for monitoring and compliance with these standards.

This has necessarily been a broad brush and, I hope short, impression of the privacy issue as consumers in Canada have identified it to our Association and of some of the initiatives we have taken on this issue. With the new technologies developing at such a rapid pace, it is imperative that Canada develop a legislative framework to ensure that the consumer's need to retain control over personal information is assured; that legislation is established to assure easily accessible methods of redress if privacy is violated, and that Canadians be made aware of their responsibilities and their rights in this field. We applaud the initiative of the Ontario Government in providing this forum on the issue. We hope it will lead to effective computer crime standards and legislation such as are necessary to provide protection which is vital to consumers in this information society.

Thank you.

PANEL 6: "TRANSBORDER DATA FLOW: TOWARD A RESOLUTION FOR THE FUTURE: THE TRENDS, THE ISSUES"

CHAIRMAN: Russell Pipe *

PANELISTS: Professor Thomas L. McPhail

Jan Fedorowicz

Jim Grant

COMMENTATOR: Peter Robinson **

---

* Mr. Pipe is President of International Business Action Centre (IBAC) in Amsterdam, Holland, and President of Transnational Data Reporting Services Inc., Amsterdam and Washington, D.C. Mr. Pipe acts as a consultant, writer and conference speaker and was instrumental in assisting the Senate Government Operations Committee and Congressman Barry Goldwater, Jr., in preparing the Privacy Act of 1974. He is Editorial Director of Transnational Data Report, published by North Holland Publishing (Amsterdam).

** Mr. Robinson is a Special Advisor on the International Aspects of Informatics in the Federal Department of Communications and has been involved in Canada's work with the OECD regarding Transborder data flow.

TRANSBORDER DATA FLOW (TBDF) AND THE CONTINENTAL COMMUNICATION PACT (CCP): THE RATIONALE FOR A COMMUNICATION PACT

THOMAS L. McPHAIL, Ph.D *
Director and Professor
Graduate Programme in Communications Studies
The University of Calgary

This paper deals with the issue of transborder data flow (TBDF)[1] with an eye toward the future. Essentially the paper reviews the major concerns with TBDF including the three most salient items, privacy, employment and sovereignty. The paper then continues to elaborate on three potential scenarios in terms of future trends and concludes with a detailed discussion of the third scenario, the Continental Communication Pact (CCP). The CCP is a proposal for a bilateral sectoral informatics pact with the U.S. that will both maximize the benefits to Canada as an information based economy as well as recognize the natural communication interconnection with the U.S. marketplace.

Introduction:

In the later 1960's and early '70's, the issue of privacy and computers was considered a "hot topic". In fact, as part of the Canadian Telecommission Studies there were a series of privacy related papers that were produced jointly by the Federal Department of Communications and the Federal Department of Justice; yet, little legislative action resulted, but at least the studies indicated an early willingness to examine the issue in terms of other countries', mostly European, initial concerns of privacy and computers. In turn, during the 1970's many of the non-economic concerns about computers were viewed through the prism of privacy.

But, in the mid 1970's, the debate shifted from privacy to freedom of information issues and access laws resulting from legislative action in various Western nations, particularly the U.S. Now once again, the issue has shifted from these areas to a more broadly based concern about "informatics". Informatics is the marriage of computers and telecommunications in such a way as to produce a blurring of traditional processes and procedures with regards to the storage and access to a multitude of data bases, particularly those controlled by transnational corporations (TNC's).

The means of affecting TBDF may be a consequence of either legislative action, such as Brazil (to be detailed later), or non-legislative action, such as economic barriers, that have the net effect of altering the flow of computerized information and access to computerized data bases. Further examples of non-legislative actions include tariffs, discriminating pricing, idiosyncratic technical standards, import quotas or government subsidies.

---

* Tom McPhail is a Professor of Communications and Director of the Graduate Programme in Communications Studies at the University of Calgary. He has worked for the Federal Department of Communications as policy advisor and consultant (1968-1972), worked on the first interactive cable project in North America with the MITRE Corporation in Washington, D.C., and acted as a senior consultant to UNESCO in Paris in the late 1970's. He has presented over 80 research papers dealing with different facets of communications and has published with Sage Publications: Electronic Colonialism: The Future of International Broadcasting and Communication.

Of interest to this Conference is the fact that privacy is now re-emerging as a major issue, not based on traditional concepts, but rather, based upon two new concerns. In this respect privacy has been "born-again" in the TBDF debate.

The first is the introduction of a large scale of private carriers that are now holding individually identifiable information, firms that are referred to as "value added" or "carriers carrier". These satellite services, either through potential competitors to Telesat, COMSAT or Intelsat, or through I.B.M.'s SBS, are collectively representing a quantum increase in the movement toward essentially non-regulated, or minimally regulated, private TNC communicating carriers.

The second development is the continuing increase, estimated 20% a year, of on-line data bases available from a diverse range of information providers and processors, including governments, businesses, and research institutes. Not only are these data bases increasing in actual numbers, but also the ability to move the data electronically between systems in diverse nation states is increasing in parallel. Although I will not deal with it here, clearly the examination of these issues by the Commission of the European Communities, plus the OECD, provide ample evidence of the European communities' concerns with the informatics and privacy.[2]

It is significant to note that European states place greater importance on privacy and national sovereignty along with other social-cultural and non-economic concerns. Solely economic or technical considerations are lower on the agenda for these nation states. To a considerable extent, the Canadian situation and public policy approach to informatics is closer to the European view rather than the U.S. view.

One could argue that in terms of the United States that national sovereignty has not been a major concern for them since they control most of the major actors in the informatics fields, Indeed their sovereignty is being enhanced by the computer revolution. Also to blindly pursue the U.S.'s deregulation strategies in the area of informatics is not in the public interest from a Canadian perspective.[3] I will come back to this later.

The concept of non-economic concerns involving TBDF is reflected in the issue of protection of privacy; particularly concerning information about individuals that has been stored in or is accessible by foreign-based computer systems. Personal files may contain a wide range of information about an individual's financial, economic, educational, welfare, business and insurance status, medical or criminal history, and political and religious beliefs. The increase and ease of TBDF heightens the concern that foreign governments, corporations or persons, may have access to this personal information. Recipients of data may have the information before the ultimate users do. Loss of control over information introduces new complexities regarding data security.

Economics & Employment

Another related concern of even more importance to Canada is the implications of TBDF on the economy of our country. A major concern is that employment opportunities are being lost, mainly because the commercial data processing is taking place in the U.S. where multi-national computer firms have their head offices. In 1978 a survey of 400 Canadian subsidiaries of U.S. companies estimated that from $300 to $350 million of computing services were imported from U.S. parent companies, and this amount was forecast to increase to $1.5 billion by 1985.

It is difficult to make accurate predictions on the composition of future employment as pertinent factors which should be examined are subject to economic vagaries on a world scale (i.e. economic growth, political unrest, labour force demographics, foreign trade movements, technological breakthroughs, or decisions of TNC's).

Real employment growth refers only to new jobs added -- not job openings. The

projected job expansion has led to the common false assumption that aggregate job growth will be biased toward high technology occupations. Creation of most jobs between 1983-1990 will lie in service related sectors with few being related to high technology sectors. Economic growth will favour middle and low level occupations with clerical and service occupations accounting for up to 40% of the employment growth.

Workers in many professions will constantly find their jobs altered by sophisticated computer technologies. Examples of this phenomenon are the increasing utilization of word processors by secretaries, bookkeepers use of computerized financial spread-sheets, the growing implementation of computerized record systems by purchasing and inventory clerks, mechanics use of diagnostic mini-computers and computerized directories employed by telephone operators.

Much automated equipment is currently paced and controlled according to centralized decisions made by managers located in the office, away from the production site. This also allows TNC's to extend and centralize their decision making procedures.

But, despite widespread automation, aggregate skill requirements have changed very little over the last two decades. Automation tends to require less operator skill after certain levels of mechanization are achieved, thus reducing skill requirements. This deskilling phenomenon is evident in the computer technology industry itself. Early computers were large and expensive, manned by programmers and operators with complex skills. As the technology evolved, the tasks and skills involved also changed.

Analysts performed the more creative, skilled tasks while programmers and coders were assigned to more tedious and routine functions. Programming became easier with the advancement of user-friendly, menu prompted packages. The new generation of office computers are designed so that knowledge of computer languages or special computer skills are no longer essential.

Office computers currently perform tasks formerly executed by secretaries, emphasizing the reduction of requisite skills needed to perform this type of office work. Word processors correct typing errors and spelling mistakes. As more advanced software is developed highly trained skilled workers will be in less demand.

A Standford study by Levine & Rumberger in February, 1983 states:

> In addition to this "deskilling" effect it is possible "that entire classes of skilled workers will disappear or be severly reduced in numbers as their jobs are replaced by robots or computer software." For example, the draftsman could easily be replaced in the not-too-distant future by widespread use of computer-aided design (CAD).

Given that most new jobs will not require higher skill levels and the probable deskilling of many existing occupations, the authors identified three appropriate education policies for the future.

The Stanford study continues:

> First, the general educational requirements for creating good citizens and productive workers are not likely to be altered significantly by high technology. Everyone should acquire strong analytic, expressive, communicative and computational skills as well as extensive knowledge of political, economic, social and cultural institutions.

Second, since it is not possible to predict the types of jobs available and selected, and the changes in jobs over a forty-year working life, general academic and vocational preparation should be stressed over specific training. Until the turn of the century, three of the five fastest growing occupations will be: data processing machine mechanics, computer systems analysts, and computer operators and they deal with high-technology products. Employment in these five occupations is projected to increase by over 100 per cent, more than four times the overall employment growth rate.

However, slower growing occupations with a large employment base are expected to contribute far more jobs to the economy than high-technology occupations. In fact, the five occupations expected to produce the most new jobs are all in low-skilled areas: janitors, nurses' aides, sales clerks, cashiers and waiters/waitresses. For example, while 200,000 new jobs for computer systems analysts will be produced in the U.S. between 1978 and 1990, over 600,000 new jobs will be created for janitors. Although employment in high-tech occupations will increase quickly in percentage terms, the contribution of these jobs to total employment growth will be small.

To put it bluntly, Canada has a vested interest in obtaining its reasonable share of computer related jobs, particularly in data processing, otherwise, as the Stanford Study indicates, we could, as a nation, wind up with a far greater and disproportionate share of the low-skilled variety of jobs.

Sovereignty

Canada has been investigating domestic communication issues for years. Yet the numerous reports and studies of public policy in all areas of communication have incited a minimum amount of action or sustained attention within the highest levels of our federal government.

One early report, Instant World: A Report on Telecommunications in Canada (1971) was compiled by a study group called "Telecommission". With the cooperation of government, industry, and university personnel, Honorable Eric Kierans, the first Canadian Federal Minister of Communications in 1969 organized a broad ranging study to examine the present and future issues in telecommunications, and to address accompaning social changes. A major observation from the study was that some Canadian information was being stored exclusively in U.S. data banks. At that time, the Canadian insurance industry relied on computerized information from Hartford, Conn. Canadian hardware-makers used a Columbus, Ohio, data bank for prices and stock quotes, and real estate information for four major Canadian cities was held in a Detroit data bank.

In addition to this early deliterious example of TBDF, the report noted that a continental system existed covering services between the U.S. and Canada. For example, telephone rates were established by the TCTS, (TransCanada Telephone System), the six member companies which shared the U.S. border, and AT &T (American Telephone and Telegraph). However, because regulatory bodies such as the CTC (Canadian Transport Commission), the Department of Communication and the COTC (Canadian Overseas Telecommunications Corporation), were not coordinated in agreements, ad hoc policies developed.

Instant World (1971:96) also addressed the issue of cultural privacy:

> This holds that cultures which may be intrinsically rich and satisfying but which are relatively weak in contemporary terms, can neither assimilate inexpensive foreign-produced media content, nor afford to produce material of equally commanding audience impact on their own.

The study recommended that Canada undertake extended R & D efforts to meet Canada's specific media needs. Other recommendations included: the development of multi-disciplinary executives in the industry for effective futuristic planning, as well as multi-lateral discussions involving governments, industry, and universities.

At the management level, the Telecommission advised the expansion of facilities to accommodate Canada's regional diversity, the integration of networks, and particularly, the development of coast to coast digital transmission systems with linked data bank and information processing organizations.

The main trust of Instand World (1971:169) is:

> To redress the balance, authorities - federal, provincial and municipal alike - may find it worthwhile to collaborate in addressing them-

selves to these problems so that the greatest possible benefits can be derived from the individual regional, provincial and national opportunities that Canadian computer/communications systems may be expected to provide with a significant impact on social, cultural, political and economic activity.

Eight years after the Telecommission study, the Consultative Committee on the Implications of Telecommunications for Canadian Sovereignty (1979), under the direction of Chairman, J.V. Clyne, submitted another report. The Clyne report asserted that Canada should work at being a leader in the field of telecommunications and that its position in the field should be a major focus of public policy. With the concern that Canadian sovereignty was being jeopardized in two fields, the Clyne report (1975:5) stated,

> First, Canadians are already being swamped with foreign broadcast programming and a new approach to the problem is urgently required; at the same time, there is a danger that foreign interests may achieve a predominant share of the market for data processing services, and far too much of the information stored in data banks will be of foreign origin.
>
> Second, Canada is heavily dependent on imports in telecommunications technology. In certain sectors, such as satellites and information exchange, Canada is in the forefront of competitive technological developments. The exploitation of these developments requires public support that does not entail a vast expenditure of public funds; this is an industrial sector that can create jobs and be competitive on an international scale.

The recurring theme in the Clyne Report was the urgent task of the Canadian government to step into the telecommunications industry with a strategy designed to both preserve Canadian sovereignty and to capitalize on opportunities in the communication industry. Issues such as broadcasting content, data flow and Canadian ownership of manufacturing and media facilities prompted the Clyne Report to recommend greater government involvement in R & D and in coordinating government and industry efforts.

In The Information Revolution and Its Implications for Canada, (1981), the complexity of communication issues was documented. Because of the fragmented nature of the Canadian economy with its foreign subsidiaries and domestically controlled firms, Canada was described as being vulnerable to conflicting interests -- regional U.S., national, domestic, U.S. foreign. Jurisdictional disputes were documented among the various levels of government, the public lacks awareness of the developing communication issues, and the small Canadian market which cannot provide a strong base for Canada's high technology and electronics industries were outlined. The author adopted the stance that the information society holds both promise and peril for Canadian society, and that government has a key role in maximizing the promise.

More recently the Science Council of Canada reiterated the issues and many of the same recommendations of these previous studies in its Report #33, Planning Now For an Information Society: Tomorrow is Too Late (1982:28). In describing the Canadian electronic industry, the report drew attention to the fact that Mitel and Northern Telecom products can compete on an international level, yet Northern Telecom is only a medium-sized company. Because of the vast amounts of government support in other countries, competition in electronics is as much between countries as companies; further, 72 of the 100 largest Canadian companies are foreign owned or controlled.

The report stated that a significant component in Canada's future should be a broadly-based chip manufacturing capability for R & D, and effective technology transfer to occur. Since Canada depends heavily on natural resources, the Science Council also recommended improved R & D into technical applications for improved productivity, particularly in the oil and mining industries where

extraction is costly. The report attributed Canada's lagging manufacturing sector to the fact that its domestic market of less than 22 million people has not promoted the growth of plants for world scale production and competition.

The Science Council recommended government support of R & D for such things as robotics and specialized computers, but in a reiteration of the rudimentary concern of the previous reports and with renewed urgency, the report (1982:53) stressed:

> The creation of a national telecommunications system to provide the infrastructure for the future cultural and economic development of Canada means that telecommunications policy development will require serious attention by the relevant provincial and federal government agencies.

Relative to a future Canadian communication policy, the report (1982:53) continues,

> If we do not develop a comprehensive telecommunications policy soon, the resulting confusion will lead to wasted resources, and loss of time in the world race to develop networks and possibly allow the entry into Canada of powerful competing networks from abroad. It is imperative that a policy be enacted designating areas of activity for existing participants, yet providing the needed flexibility to accommodate new competition and the emergence of new technologies.

Both historically and recently sovereignty and other non-economic concerns have been high on the government agenda with reference to the emerging Information Age.

Whatever implications TBDF may have on Canada, the U.S. has recently indicated a willingness to discuss initiatives on sectoral free trade; among the sectors under consideration is informatics. With both countries committed to the multilateral GATT trading system, bilateral agreements will require special handling.

The U.S. has called for cooperation in expanding trade and investment, for the removal of such irritants as the America-Buy Canada provisions, for reducing uncertainties about access, and for removal of other non-tariff barriers. Yet recent U.S. government hearings regarding the steel industry call into question the de facto call for "free trade". U.S. government quotas on Japan auto imports is another example of not so "free trade" approaches when the U.S. perceives itself (or its voters) to be adversely affected.

Essentially pursuing the status quo with regard to TBDF, or even a modified status quo, will continue to see ad hoc policies and policy by incrementalism ultimately resulting in the U.S. being in a favorable or priority position. This is for two major reasons. The first being simply the size, and quickness with which the U.S. government responds in its own vested interests; second, many of the institutions and industries affected by any negotiations are either highly interconnected within the U.S. market or, in fact, are corporately controlled by American parent firms.

Therefore the net result of any continuation of simply relying upon a sectoral approach that responds merely to irritants or to points of conflict will simply see a gradual decline in the Canadian position in the long run. This is true in the three major areas discussed previously, namely, privacy, employment and sovereignty.

Options

What then, are the options? If the status quo or a modified status quo and incrementalism are not in the national interest, what other actions may be taken? Well, we may look to the example of Brazil. It is a negative model yet it deserves examination to determine if their model or approach may be applicable to the Canadian situation. Once I have described in some detail the Brazil response to the issues of informatics, privacy, computers and TBDF, I will then spell out a new Canadian option.

TABLE 1

PERSONAL PRIVACY REGULATIONS & ISSUES	AUSTRALIA	AUSTRIA	BELGIUM	CANADA	DENMARK	FINLAND	FRANCE	HUNGARY	ICELAND	ISRAEL	JAPAN	LUXEMBOURG	NETHERLANDS	NEW ZEALAND	NORWAY	PORTUGAL	SPAIN	SWEDEN	SWITZERLAND	UNITED KINGDOM	UNITED STATES	WEST GERMANY		EEC	COE	OECD	IBI
A. TYPE OF REGULATION	LP	L	LP	L	L	LP	L	LP	L	L	R	L	LP	L	L	LP	LP	L	LP	R	L	L		R	R	G	R
B. PROTECTED PERSONS - Natural Persons	X	X	X	X	X	X	X			X		X	X	X	X		X	X		X	X	X		X	X	X	
Citizens/Residents Only				X																	X						
Legal Persons		X	X		X							X		X	X										X		
C. NAME-LINKED DATA--EDP/ADP	X	X	X	X	X	X	X			X		X	X	X	X		X	X		X	X	X			X		
Manual Data Processing	X	X		X	X		X						X		X		X				X	X			X	X	
Collection/Flows/Storage	X	X				X	X			X		X		X				X						X	X	X	
D. CONTROL - DATA Control Boards		X	X	X	X		X					X	X		X		X	X		X		X					
Registration/Licensing		X	X	X			X			X		X			X			X			X	X					
E. RIGHT TO ACCESS/CHALLENGE	X	X	X	X	X		X			X		X		X	X			X			X	X			X		
Freedom of Information	X	X		X	X	X	X					X	X		X			X			X	X					
F. LEVEL OF GOVERNMENT - Local	X			X													X		X		X	X					
National	X	X	X	X	X		X		X	X		X	X	X	X	X	X	X			X	X					
International					X									X	X			X						X	X	X	X
G. REGULATED SECTOR - Public		X	X	X	X		X					X		X	X			X			X	X		X	X		
Private		X	X		X		X					X			X			X				X		X	X		
Self-regulation						X																X					
H. ENFORCEMENT Fine							X					X									X						
Victim Compensation														X	X												
Data Confiscated/Destroyed			X									X						X									

KEY

LP: Legislation - Pending
L: Legislation - in Force
R: Report
G: Guidelines
EEC: European Economic Community
COE: Council of Europe
OECD: Organization for Economic Corporation & Development
IBI: Intergovernmental Bureau for Informatics

Note: The countries studied differ in degree of "regulatedness" or in strength of laws and diligence of enforcement. An "X" simply denotes the existence of a condition, not its strength.

Source: Transnational Data Report 1978-1983, Vols. 1-6; EEC, COE, IBI REPORTS, OECD Guidelines and personal correspondence.

Table 1: Transborder data flow, data protection, and privacy regulation in 22 nations

In Brazil, the government believes that it does not want to become a "computer colony"[4] and this has led, over the last decade, to a complex network of regulations administered by the Special Informatics Secretariat. Brazil sees independence in computer technology as a matter of sovereignty and national pride, plus the government has taken strong steps to insure the development of a broadly based domestic informatics industry. Nationalism was in fact present at the birth of Brazil's computer industry when, in the mid 1970's, the country's Naval Ministry demanded the security for its computer systems installed in its frigates and destroyers.

As a result, the entire issue was taken up by the military government's National Security Council. In 1977 it sponsored the creation of a state computer company, Cobra, and two years later formed the Special Informatic Secretariat, headed mainly by army and navy engineers.

Since then, an alliance of military officers, local entrepreneurs, and leftist cultural nationalists has formed a coalition around the ideal of protecting and enlarging the emerging Brazilian computer industry. Foreign-owned subsidiaries, principally I.B.M.,[5] have decreased their total share of the market. In five years their share has fallen from 77 per cent to 53 per cent. Since 1979, domestic sales of Brazilian-made computers has gone from 200 million to almost 700 million. Sales of imported computers have decreased from a high of almost 300 million in 1981, to less than 100 million in 1983.

Brazil's Congress is now debating a law to govern informatics policy, plus the government wants to eliminate the confusion caused by the plethora of ad hoc regulations. No matter what the ultimate decision of Brazil's government will be, the figures indicate that blocking imports has helped the local industry thrive. The government's strong steps have insured the development of a domestic informatics industry. The net losers are the foreign TNC's.

There has been other activity as well. Among the actions that have been taken internationally are OECD's "Guidelines Governing the Protection of Privacy and the Transborder Flow of Personal Data" (Sept. 1980). The Council of Europe adopted a "Convention for the Privacy of Individuals with Regard to Automatic Processing of Personal Data". In the case of non-personal TBDF, according to the center on Transnational Corporation, about 60 countries have issued some official statement.

Another example is Sweden which has operated its Data Inspection Board since 1974. Data banks containing information about the acitivities of individual citizens may not be constructed without permission of the "inspectorate". If any personal information is intended for use outside Sweden, its issuance depends on special permission.The trend towards increased data regulation, particularly in Europe, will both ultimately and indirectly affect TBDF in other countries.

A Continental Communication Pact (CCP):

Reports, studies, and commissions attempting to address the TBDF issues have failed to come up with clear-cut Canadian strategies. Questions of privacy, competition, technical change, and regulation on a multi-lateral basis add to the complexity of policy making. In order to deal effectively with the TBDF problem, and in order to be more realistic, the issues should be broken down into something more manageable; such as a single bilateral TBDF agreement with Canada's trading partner - the U.S.

Key assumptions are fundamental to the approach of policy making on the TBDF question. Canada's conviction is that enormous benefits can come with the increases in TBDF. It has been suggested that in order to capitalize on the opportunities in the industry, telecommunications policies should be developed so that Canada can gain entry into the powerful competing networks in the U.S. Interruptions in flows of data between our borders could have negative implications to the computer service industry and almost all industrial activity in

Canada. If trade in data, information, and associated services is to proceed smoothly, Canada must resist temptations to become protectionist. We do not want to become Brazil North.

In establishing a "Continental Communication Pact" (CCP) with the United States, Canada and the U.S. would do well to examine the Auto Pact Agreement of 1965. That agreement was signed to provide duty-free trade by manufacturers in automobiles and parts between the U.S. and Canada. At the time of the Pact, Canada's position in the automobile industry was weak; it was incapable of competing in an international market because of the expense to duplicate U.S. cars in Canadian subsidiaries. The Auto Pact promised to redress the deficit in the sectoral balance of trade and expand production in Canada.

Recently in discussing U.S./Canada economic relations, U.S. Deputy Assistant Secretary of State, James Medas stressed that the Reagan administration is firmly committed to the promotion of freer trade. Last month, Canada and the U.S. signed a safeguard understanding to help assure prompt consultation and cooperation on shared trade concerns. The stage is now being set for a CCP to be established. The U.S. Government has stated a variety of sectors under consideration to the recent Canadian initiative on sectoral free trade, informatics being one of them.

Let us examine the CCP in more detail.

First, the CCP will involve broadcast, telecommunication and computer services/supplies.

Second, it will involve a continental communication grid involving the national governments of the United States and Canada.

Third, communication stakeholders (both public & private, including provincial governments) should be consulted prior to the formation of a CCP.

Just who are the stakeholders. A sample list follows:

- Computer firms
- Telesat Canada
- TCTS & CNCP
- Provincial telephone companies
- Cable companies
- Canadian independent film producers/Telefilm
- National magazines
- Hardware suppliers and manufacturers, e.g.Mitel, Northern Telecom, NABU, etc.
- Software suppliers - information providers, e.g. Infoglobe
- Pay TV distributors
- Advertisers
- Financial community
- Investors
- Governments - relevant federal and provincial departments
- Labor unions

A few words of explanation. Today we have a series of ad hoc and disjointed, short-run and frequently conflicting policies. In addition, the federal government's involvement frequently fails to take into account either the provincial role or perspectives.

Meanwhile, DBS, cable, videotex, mobile radio and TBDF are growing on a continental scale precipitating interrelated policy concerns. The CCP would broaden the market for Canadian products, both hardware and software, so as not to be swamped by foreign mostly American products. To have the CBC and CTV carried on all U.S. cable systems, or new pay service(s) carried on U.S. satellites would financially aid the Canadian services and redress the current imbalance. In addition, it would provide guidelines for Canadian cable companies such as Rogers, Maclean-Hunter, Cablecasting, etc., with franchises in the U.S.

The U.S. networks are carried on Canadian cable systems and U.S. pay services are being received by a growing number of Canadian-based earth stations (TVRO's); now the major question is why not have a reciprocal agreement to benefit Canadian manufacturers and software merchants.

A major indicator of Canada's need to develop a communication pact is the trade deficit in computer and office equipment. Chevreau (1983:B 5) indicates that, in 1982, Canada's trade deficit passed the $2 billion level; exports totalled $890 million while imports of computers totalled $3 billion.

In spite of government efforts to reduce the deficit through sales of Telidon or Office Communications Systems, Evans Research Corp. of Toronto predicts the deficit will grow to $5 billion by 1986. The trend towards office automation has increased Canada's demand for foreign office electronics equipment. DOC's throwing a few dollars into office automation projects only masks the more serious underlying structural problems.

There is a greater hope for the marketing of Canadian programming in the U.S. albeit the demand is not yet proven. From the CBC Annual Report (1981-1982), it is apparent that a market does exist for Canadian products, particularly those relating to the arts, in addition to the news programs, As It Happens and Sunday Morning. These have set the precedent for the possibility of a greater Canadian presence in the American communications scene. An information pact would outline the strategy for the promotion of CBC, NFB, CFDC or Telefilm productions on American networks and theatre screens.

With regards to satellite technology, Canada is being forced into a pact with the U.S. over the issue of future DBS services. Both Canada and the US. are seeking to reserve prime satellite orbital slots for future use. While the FCC is planning to establish a DBS system with up to 13 services, Canada is requesting 6 slots with full frequency bandwidth of 500 mhz reserved for each service. Canada's request raises the problem of maximum spacing between each satellite which will be necessary to accommodate the proposed Canadian services, yet it will also mean that the U.S. will be left with only 4, mainly unfavorable slots. Negotiations will require adjustments to the requests of both countries, although the U.S. favors a system where applications are granted on expression of demand and first-come first-served.

Yet once again, Canada is demonstrating concern for the preservation of its sovereignty by seeking an orbital slot for each of its five time zones and an additional slot for French programming for Quebec. While Canada does not have the economic resources to develop these services immediately, it is seeking to prevent the U.S. from absorbing all the available slots now. (It is to be remembered that other smaller countries, particularly in South America, are hoping to use DBS services in the future, and are looking at the same parking spaces that Canada and the U.S. are hoping to capture.)

Another example of the informal movement toward a CCP is a recent agreement between DOC & NASA to establish a cooperative effort to define a single space programme to meet mobile communication needs in both countries. This joint effort may result in a common mobile satellite system offering similar services in both countries.

The issues of both content and hardware/software sovereignty could be addressed by the negotiation of a joint satellite serving both the American and Canadian public. Canadian strategy on this point would involve a bilateral agreement with the United States regarding the division of revenues from the joint satellite network; the equity of content/carrier status, and the equal division of American and Canadian programming services provided by the satellite, plus shared R & D. The R & D aspect will protect Canada from becoming a technological serf in the Information Age.

A final point. This CCP proposal is aimed at strengthening Canadian cultural industries; the status-quo requires writers, producers, directors, etc. to continually water-down Canadian references, history, themes, etc. to accommodate U.S. commercial concerns. With the CCP the carriage would be guaranteed and therefore a Canadian perspective dealing with Canadian ideas, norms, perspectives, etc. (like the Australian film

industry) will be possible. The CCP is not aimed at a mass audience philosophy but rather is consistent with the narrow casting or tiering approach of evolving North American cable-satellite hybrid systems.

Without such a bold enterprising move as the CCP, Canada will lose its already weak position with regards to hardware technology and software. The status quo is really a closet policy giving Canada the worst of both worlds (hardware and software). Ad hoc policies are not sufficient to guarantee a significant Canadian presence in the international and continental scene, and market forces have historically indicated that American programming has a significant edge over Canadian production prospects. Therefore, the urgency to develop a CCP with the United States is increasing and it is up to Canadian policy-makers to explore the opportunities in order to secure Canadian privacy, sovereignty, and employment opportunities in the Information Age.

Conclusions

In sum, this paper has reviewed the area of TBDF through the prism of privacy, in part, with additional concern for the areas of employment and national sovereignty. Also discussed were three models of approach for future action in the area of TBDF.

First, an examination of the status quo, or modified status quo, which will see the Canadian position deteriorate over time in favor of both the U.S. government position as well as for the benefit of the commercial and corporate interests of U.S. communication industries was discussed.

Second, an examination of a restrictive TBDF model, particularly in Brazil, was examined as well as outlining their rationale and actions in terms of the general area of informatics.

Third, a new plan was outlined and elaborated upon dealing with a Continental Communication Pact (CCP). The CCP was outlined in terms of the various stakeholders involving broadcast, telecommunication, and computer firms.

In addition, examples were cited to demonstrate the range of issues, a possible procedural approach involving both the public and private sector as well as provincial governments, and finally, comments were made concerning the ability of the CCP to both enhance and enrich the cultural sovereignty of Canada as a nation state, as well as provide for a more equitable distribution of research and development for future communication technologies, plus some enhanced likelihood of additional manufacturing jobs being available in Canada in the high technology area.

Endnotes

1. For the purpose of this paper "transborder data flow may be defined as the transmission of machine readable data and information over trans national computer and other electronic communication systems for the purpose of storage, retrieval, or processing". "Transborder Data Flow, Informatics, and National Policies", Journal of Communication, Winter, 1984, p.154.

2. The OECD data declaration will be discussed in Paris on July 2-3, 1984 by the OECD Working Party on TBDF.

3. It is somewhat ironic that in 1984 the nation with the greatest investment in international communication affairs, the United States, is also the same nation that is doing its utmost to close down those international fora or associations that are most likely to aid it in its goals, whatever they be, whether it is free flow of information, TBDF, or free trade, or rational and efficient use of the international spectrum space.

Consider the following that points the accusing finger at the Reagan administration for manipulating U.S. policy and participation in international communication affairs in a deleterious, disruptive and negative fashion.

"U.S. Off Course

On the contrary, the U.S. is moving in the reverse direction, abandoning or neutralizing a forum capable of accommodating a broad, varied membership and of accepting revised agendas and new perspectives. The U.S. proposes to leave the United Nations Education, Scientific and Cultural Organization (UNESCO), partly because of its attention to disputed international communication practices and conditions. The U.S. is pressing the International Telecommunication Union no less (ITU) to confine itself to technical concerns. It is reducing its participation in the U.N. Committee on Information and in the legal and technical sub-committees looking at future spaces communications for the Committee on the Peaceful Uses of Outer Space. It stands apart from the Intergovernmental Bureau on Informatics (IBI) and the U.N. Center for Transnational Corporations, both of which exhibit deep interest in transborder data flow problems involving the Third World." Chronicle of International Communication, April, 1984, Volume 5, Number 3, page 7.

4. For detailed discussion see: T.L. McPhail, Electronic Colonialism: The Future of International broadcasting & Communication, (Beverly Hills, Calif.: Sage Publications, 1981). Also refer to other writings by the same author listed in the bibliography.

5. I.B.M. also has some domestic (U.S.) critics.

"Moreover, given I.B.M.'s recently demonstrated litigiousness with its smallest opponents, would be competitors have experienced a deep chill, especially if there are former I.B.M. employees. The danger is that a class of 'technological serfs' is being created -- those who once worked for I.B.M. are now forever subject to trade secret litigation. It is a disturbing paradox that, now freed from (U.S.) government litigation, I.B.M. is using litigation to stifle competition and block the diffusion of technology in elevation, especially in the main frame plug-compatible markets." New York Times, Sunday, May 13, 1984, page 2F.

6. I will not discuss the details or results of the auto-pact here, but Beigie (1970) and others have studied it elsewhere.

References

Beigie, Carle E. "The Canada-U.S. Automotive Agreement: An Evaluation." Canadian American Committee, Canada. 1970.

"Brazil's Prickly Computer Policy". The New York Times, April 29, 1984. p. 12F.

Chevreau, Jonathan, "Computer, Office Equipment Showing Higher Trade Deficit." Globe and Mail, February 11:B5, 1983.

Clyne, J.V. "Telecommunications and Canada, Consultative Committee on the Implications of Telecommunications for Canadian Sovereignty." Minister of Supply and Services, Canada. 1979.

"Council of Europe Convention for the Protection of Individuals with Regard to Automated Processing of Personal Data." Transnational Data Report 3(6), 1980.

Crawford, Morris H. "The IBI Transborder Data Flow Conference: An American View." Transnational Data Report 3(3-4), 1980, pp. 38-41.

Cundiff, W.E. and Mado Reid, "Issues in Canadian/U.S. Transborder Computer Data Flows." Institute for Research on Public Policy, Toronto: Butterworth & Co. Canada, Ltd. 1979.

European Communities, Commission. "European Society Faced with the Challenge of New Information Technologies: A Community Response." Brussels: European Economic Community, 1979.

"Europe/North America: A One-Way Flow." Information Systems 30, 1979.

Ganley, Oswald G., "The United States-Canadian Communications and Information Resources Relationship and Its Possible Significance for Worldwide Diplomacy." Program on Information Resources policy, Working Paper, Cambridge, Mass.: Harvard University. 1979.

Hamelink, Cees J. "Informatics: Third World Call for New Order." Journal of Communication 29(3), Summer 1979, pp. 144-148.

The Impact of Transnational Data Flows on Developing Countries. J.C. Grant. An address to the Conference on Information, Economics, and Power North South Dimension. The University of Western Ontario, School of Journalism. March 10, 1984.

Instant World, "A Report on Telecommunications in Canada", Ottawa: Information Canada. 1971.

Issues in Canadian/U.S. Transborder Computer Data Flows. W.E. Cundiff and Mado Reid (Eds.) Proceedings of a conference sponsored by the Institute for Research on Public Policy. 1978.

Lesser, Barry, "The Implications of the Federal and Provincial Proposals for Regulating Telecommunications: An Economist's Perspective, in Telecommunications Regulation and the Constitution." Robert Buchan, Christopher Johnston (Eds.) Montreal: The Institute for Research on Public Policy. 1982.

Lester, R.M., "Communications and Transborder Information Flows." The Conference Board of Canada Business Outlook Conference, unpublished paper. 1981.

Levine, H., & Rumberger, R., Stanford University, Project Report No. 83-A 4.

McPhail, Thomas L., "The Future of Canadian Broadcasting: Proposed Revision of Regulatory Mechanisms and Policies", in The Crisis in Canadian Broadcasting. (Ottawa: Canadian Broadcasting League, 1976).

McPhail, Thomas L., "Electronic Colonialism: The Future of International Broadcasting and Communication. (Beverly Hills, Calif.: Sage Publications, 1981), pp. 259.

McPhail, Thomas L., "Telematics, Telejournalism in Public Policy Concerns", Competition in the Information Economy, Horizon House, 1981, pp. 417-420

McPhail, Thomas L., "The Future of Canadian Communications", Communications in Canadian Society, B. Singer, (ed.) Toronto: Addison-Wesley 1983, pp. 73-82.

McPhail, Thomas L., "Direct Broadcast Satellities: The Demise of Public and Commercial Policy Objectives", Telecommunications in the year 2000: National and International Perspectives, (with S. Judge), Indu Singh, (ed.) (Ablex Publishing Corporation, Norwood, New Jersey, 1983), pp. 72-79.

Medas Points Directions in U.S./Canada Economic Relations. James Medas, U.S. Deputy Assistant Secretary of State. Text of Speech delivered in Montreal to Canadian Club of Montreal, The Chambre de Commerce du District de Montreal, and the Montreal Board of Trade. March 19, 1984.

Melody, William, "Are Satellites the Pyramids of the 20th Century?" In Search, Volume VI, No. 2 Spring pp. 2-9.

Organization for Economic Cooperation and Development. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris: OECD, 1981.

Planning Now for an Information Society - Tomorrow is Too Late. Science Council of Canada - Committee on Computers and Communication. 1982.

Read, William H. "Foreign Policy: The High and Low Politics of Telecommunications." In Anthony G. Oettinger, Paul J. Berman, and William H. Read (Eds.) High and Low Politics: Information Resources for the '80s. Cambridge, Mass.: Ballinger, 1977.

Robinson, Peter. "Some Economic Dimensions of TDF." Transnational Data Report 3(3-4), 1980, pp. 18-19.

Schiller, Herbert I. "Computer Systems: Power From Whom and From What?" Journal of Communication 28(4), Autumn 1978, pp. 184194.

Science Council of Canada, "Planning Now for an Information Society: Tomorrow is Too Late." Minister of Supply and Services, Ottawa. 1982.

Serafini, S. and M. Andrieu, "The Information Revolution and Its Implications for Canada." Communications Economics Branch, Department of Communications, Minister of Supply and Services, Ottawa. 1980.

Silverman, Paul E. "The Evolving Market for International Communications." Telecommunications, April 1978, pp. 25-30.

"Survey Shows 35 Countries to Regulate Data Flows." Transnational Data Report 1(7), 1978.

Telecommunications and Canada. Consultative Committee on the Implications of Telecommunications for Canadian Sovereignty.

"Trade Barriers to Telecommunications, Data and Information Services." Transnational Data Report 5(4), 1982, pp. 179-185.

Traded Computer Services: A Bilateral Beginning. An address by Rowland C. Frazee, Chairman and Chief Executive Officer, The Royal Bank of Canada. Delivered at the Bookings Institution Washington, D.C. April 10, 1984.

Transborder Data Flow a Hot Issue. Lawrence Surtees, Globe and Mail, February 24, 1984.

Transborder Data Flows: A Multinational Issue. C.J. Maule. An Article appearing in the Foreign Investment Review, Autumn 1982.

Trubow, George B. "Privacy, Policy and Computers." Paper presented to the Computer Privacy and Security Symposium, "Top Secrets 1981," sponsored by Honeywell Information Systems, Inc., Phoenix, Arizona, April 1981.

Wigand, Rolf T. "Direct Satellite Broadcasting: Selected Social Implications." In M. Burgoon (Ed.) Communication Yearbook 6. Beverly Hills, Cal.: Sage, 1982, pp. 250-288.

Wigand, Rolf T., Shipley, C. & Shipley, W., "TBDF, Informatics, & National Policies", Journal of Communication 24(1), Winter 1984, pp. 153-175.

Williams, J.K. "European Data Protection - A business Viewpoint." Transnational Data Report 5(3), 1982, pp. 156-157.

TBDF AND THE SHAPE OF A CANADIAN-AMERICAN INFORMATION AGREEMENT: PROBLEMS AND PROSPECTS

J.K. FEDOROWICZ *
Manager, International Policy
Canadian Chamber of Commerce

The technological revolution in electronic information systems and telecommunications has made possible the emergence of the first truly global economic system in human history. As ever larger amounts of information move across borders, increasing numbers of scholars, officials and business people are turning their attention to the implications of transborder data flows (TBDF) for sovereignty, national security, cultural integrity, proprietary rights, legal structures and the regulatory environment.

This has been going on for over a decade but the issue has taken on a particular kind of urgency for Canada as this country contemplates the possibility of entering into some kind of a trade liberalization agreement with the United States that would involve, among others, the 'informatics' sector.

It is not necessary to recall in this place the reasons behind attempting a somewhat awkward compromise between the status quo and the politically unpredictable course of full free trade. Suffice it to say that the Canadian government recognizes the seriousness of Canada's current economic plight and is willing to attempt unconventional remedies to advance the structural adjustment which the country needs. Securing access to the huge American market, even if only in a few important sectors, might help some industries to become competitive on a world-class basis, and if successful, it might assuage some nationalist fears of surrender to complete American domination.

Given the political minefield the Canadian government had already entered by initiating sectoral trade liberalization discussions with the United States, the inclusion of 'informatics' as one of the sectors promised to make an already complicated set of negotiations much worse. After all, it is difficult enough to define a specific sector, decide who should choose the sectors to be liberalized, establish a negotiating structure which takes all interests into account, and deal effectively with non-tariff as well as tariff forms of protection. But adding the ill-defined and quickly changing sector of informatics to the discussion ensures that the talks will be long and difficult, indeed to the point that one must question if there is sufficient political will on both sides to bring them to a successful conclusion.

It is generally agreed that adding informatics to the discussion was a suggestion which came from the American side. The United States is less concerned with the Canadian market as such, and more with the example that such an agreement would have for its remaining

---

* Dr. Federowicz currently holds the position of Manager, International Policy, for the Canadian Chamber of Commerce. Part of his responsibilities include managing the meetings and agenda of the Committee on Transborder Flows of the International Business Council of Canada. This has involved research and the preparation of background materials and position papers on transborder data issues. He has written two books as well as numerous articles, pamphlets and reviews. He has been Associate Research Director at the Canadian Institute of International Affairs since 1982.

trading partners. As the United States yields the competitive edge in traditional forms of manufacturing to newly industrialized countries (NICs), it has increasingly come to emphasize its comparative advantage in information technology and the trade in services which depends so much on that technology. Yet here too, the United States is being denied access to foreign markets by protectionist measures seeking to provide a climate in which smaller or less developed economies can nonetheless establish their own information industries and survive competition from the outside.

A mutually satisfactory agreement liberalizing trade in information-related goods and services between Canada and the United States would demonstrate that it is possible for a large and small economy to coexist to the advantage of both and this might have an exemplary impact on American trade objectives elsewhere.

For Canada, a trade liberalization agreement in informatics would also confer certain benefits. It would open up a huge and sophisticated market to Canadian hi-tech companies. It would force those companies to become world-class and those which did so could compete anywhere on the globe. And it would give Canadians access to the latest technology at cheaper cost, thus raising living standards and promoting economic growth.

Before such a happy vision can actually come to pass, however, there are a host of problems which need to be solved, or at least considered. Perhaps not all of these problems can be solved, but in raising the issue for discussion, the sectoral trade liberalization exercise will force us to think harder and deeper about some of the implications of TBDF.

Perhaps the most basic issue which demands resolution is the question of information as property. It is quite clear that computer hardware is property, and there is an increasing recognition that software too deserves patent protection, but what of the raw data assembled by computer, carried by telecommunications systems, and processed according to the software? Can one hold proprietary rights to data? If not, then it will be impossible to protect data banks (and privacy) from penetration. If data is held to be property, then governments seeking additional sources of revenue might be tempted to tax it.

If governments do attempt to tax data, then the method of valuation becomes critical. The obvious difficulty here is that the value of information depends entirely on its context, and schemes of valuation which simply measure the volume of a stream of digits are inherently absurd not to say unfair. More sophisticated attempts to tax data by encoding it before transmission add bureaucratic complexity but do not change the basic fact that the value of data is impossible to establish with any precision and attempts to do so in order to tax it will only inhibit trade and add to confusion.

One interesting feature of current attempts to tax data is that they generally depend on the data actually moving from one place to another: no one has seriously proposed taxing data stored quietly on a disk somewhere. But if moving data is liable to taxation, there is no logical reason why that process should be restricted to data moving across a border - it could with equal justice be applied to data moving within a country as well. At that point the monitoring required would be so horrendous as to undo much of the efficiency which the modern technology originally created.

To add one final wrinkle, there are those who argue that data subjects have some proprietary rights to the information about them. The argument for protecting privacy is based on this notion, as are demands from LDCs that they have access to satellite information about their resources. If indeed this proprietary claim is upheld, then surely reason demands that such co-owners of information also share any tax burdens levied on it.

The arguments presented above may seem somewhat tortured to the pragmatic mind,

but it is precisely on such arguments that court judgments are based and with -out prior clarification of definitions and principles, any international agreements attempting to liberalize trade in information will only serve as the prelude to endless litigation. In the case of sectoral trade liberalization between Canada and the United States, proprietary rights to information stored in the other country would have to be guaranteed and tax treatment on both sides of the border would have to be harmonized.

The questions of proprietary rights is only the beginning of a long and involved set of issues emerging from the TBDF discussion. If indeed information is classified as a form of property, how can that property be legitimately protected from theft, destruction, or unauthorized access. This becomes a much more serious problem in the event that an Integrated Digital Services Network is created. Some countries have opted for specific technologies or unique standards as a means of protecting themselves, others have chosen complex security specification procedures for hardware and software. Such measures can however inhibit trade in information so that a fine line between protection and efficiency must be defined and adhered to.

Given the increasing quantity of data stored in electronic form, it is inevitable that courts will have to admit electronically recorded information for evidence in court, for documentation of transactions, and for authentication. Any trade agreement liberalizing information exchange will have to be preceded by some agreement as to the reciprocal admissability of electronic evidence in court, and when the court system is complicated by several levels of government, and variations from state to state or province to province, the chances of securing such an agreement dim perceptibly.

The previous point is an important one inasmuch as any trade agreement will be challenged or tested in the courts sooner or later. For example, the question of legal liability is sure to arise in the event that damage to a system is caused by the transmission of a defective program or data. How is the source of the defect to be traced? Who is liable for damages and for what amount? Is the case to be considered negligence, breach of contract, breach of warranty or product liability? And here too, can we be sure that all state and provincial courts will treat data in the same way?

To add to these legal complications, there are also political ones. In many parts of Europe, for example, there exist centralized, state-owned Post, Telegraph and Telephone agencies (PTTs) which are fighting private business tooth and nail to retain a monopoly over telecommunications services. For the PTTs, the objective may be to use its monopoly position to ensure a certain minimum social objective such as providing cheap and universal telephone service. The objectives of business, on the other hand, are to establish private lines or leased circuits which could serve its needs far more cheaply while ensuring the privileged and confidential nature of business communication.

A similar struggle is likely to emerge in Canada where Canada Post, CN/CP, and the telephone system, though not amalgamated into a single PTT, nonetheless enjoy regulatory protection of their monopolies. That protection is currently being challenged by Canadian competitors, but the challenge will become quite dramatic if an attempt is made to liberalize information trade between a relatively regulated Canadian environment and a United States which is moving decisively in the direction of deregulation.

It is a fair question as to whether Canada's regulated monopolies will be able to compete effectively against the electronic service 'supermarkets' arising south of the border. At the very least, they too may have to expand beyond the range of services their regulations currently allow and in that case one may well ask whether it is wise or safe to permit such giant, multiservice monopolies to mushroom.

One final and inevitable legal problem exacerbated by the increase in TBDF is

that of conflicting legal requirements brought about by extraterritorial application of the laws of one jurisdiction to the territory of another. This has already been an irritant in relations between Canada and the United States, especially because of the problems the Bank of Nova Scotia encountered in trying to satisfy the demands of Florida courts which ordered the surrender of documents held in the Cayman Islands which the government of the latter forbade the bank from producing. At the very least, laws which prevent the transmission of data to countries which lack the privacy protection of the country of origin may be held to have some extraterritorial effects. There are also demands from multinational enterprises that their global operations be open to scrutiny by tax officials (unitary taxation) or labour unions (the European Vredeling proposals) in a particular country where they may only have a small proportion of their total holdings. It is likely that the problems of extraterritoriality will increase in the future and it is to be expected that in a country as prickly about its sovereignty as Canada, this will be an important component of any trade liberalization talks with the United States. The latter will have to abstain from any hint of extraterritorial application of American law if it wants Canada to enter into an agreement.

The converse of the extraterritoriality issue mentioned above is the need for some harmonization, at least in the regulatory environment. It is not likely that trade can be liberalized much between countries with different regulatory environments, tax systems, standards, and even measuring systems. Certainly trade can and does pass between them, at hugh volumes, but such differences in regulatory treatment will exact their toll. At the very least, it is to be expected that Canadian companies confined by strict regulations may find it difficult to compete against American firms operating under no such constraints.

Those who negotiate a trade liberalization agreement in information between Canada and the United States will have to be aware of walking a fine line between resisting extraterritoriality while encouraging harmonization wherever feasible. This will not be an easy task and we should not become too impatient if it takes a long time.

All of the problems listed above are of a juridical nature and they do not even begin to address the thornier political issues of cultural integrity, national security, and human rights. They are highlighted here not to discredit or decry the sectoral approach, but simply to point out the potentially huge set of issues which such negotiations will call forth. The fact that they will have to be addressed at all marks a form of progress in consideration of TBDF issues and the solutions which Canada and the United States reach in the process, may serve as useful examples to other countries attempting similar agreements.

Such solutions may prove to have a great value in turning back the protectionist tide currently seeming to engulf trade in information. Countries with a less developed information industry fear the asymmetry in their relations with technologically developed societies, and they fear being shut out of the information revolution and relegated to being the proverbial 'hewers of wood'...

If information is to be the great equalizer in the economy of the future, then even small countries want to secure their share of that industry and hence their recourse to discriminatory pricing, local content requirements, restrictions on access to closed information systems, limits on the types of equipment available to users, restrictions on modes of transmission, and restrictions on market entry, to name but a few protectionist measures which reduce the volume of TBDF and inhibit the information trade.

Businessmen argue that some kind of dramatic progress is needed to break up what is fast becoming a log-jam in the international flow of information. Just as the unprecedented economic boom of the 1950's and 1960's occurred along with progress in the GATT in eliminating tariff barriers, so too it is argued an-

other GATT round devoted to the trade in services and to non-tariff barriers may have the same salutary effects.

Yet it is obvious that the number of participants in the GATT has grown, as have the differences in their levels of development and their philosophical outlooks. We cannot expect quick and easy progress in this forum, though here too, a viable Canada-U.S. agreement may have a healthy exemplary effect, particularly if it is cast in a form which could easily be expanded into a multilateral agreement.

Because of the potential importance of a Canada-U.S. agreement in information trade, it would be advisable to proceed with care and with the appropriate consultations at every step. That means, of course, adequate input from the private sector, whose technological innovations and applications, after all, are driving forward the increasing use of TBDF. This is not to say that the voice of business should be the only one heard, but it is an important partner because of its familiarity with the technology.

The business community would probably agree on several general principles as it formulates what it would like to see in any Canada-U.S. agreement. Among those principles are the following:

- the exchange of information is vital to technological progress and economic growth
- business organizations should have the right to communicate with themselves (ie. between branches) and with each other
- we must recognize the global interdependence of communications networks: restrictions in one part will have a multiplier effect on other parts of the system
- liberalization of the trading environment cannot occur without liberalization of the conditions under which the exchange of information occurs.

Armed with such general principles, the business community would look to an agreement between Canada and the United States which would enshrine such an approach and flesh it out with concrete solutions to more specific issues. Among those issues are the following:

- the right of presence, or the right of access to information resources which would imply some guarantee that companies could connect to networks, receive data, transmit data, or receive services across borders
- some guarantee of national treatment, particularly in areas such as government procurement
- would most-favoured nation status be offered to third parties under a bilateral Canada-U.S. agreement on a reciprocal basis, ie. that treatment mandated by the agreement could be applied to third parties if they agreed to treat Canadian or American companies in the same way?
- would the United States recognize the tremendous advantage which U.S. Defense Department and NASA procurement confers on the American information industry and agree either to strictly national treatment of Canadian companies, or some compensatory advantages such as tax relief or subsidies for Canadian firms excluded from U.S. procurement?

In general, non-tariff barriers to trade in information are probably far harder to define or remove inasmuch as they can easily get confused with issues such as national security or cultural integrity. What makes the entire problem that much more difficult is that information in and of itself is not a sector in the same way that the computer manufacturing industry is clearly a sector. Information is an input or an intermediate good which affects the productivity and performance of virtually every other sector in the economy.

Consequently, negotiations on how to treat trade in information may involve consultations with a wide variety of economic sectors, not just the computer manufacturers and data processors that

would seem at first glance to be the obvious interlocutors in the process. The linkages between and among economic sectors become a critical element in determining the impact of any trade liberalization agreement between the two countries.

If the private sector expects to be treated seriously in this process, then it must be sure that its input represents the best and most thoroughly documented expertise available to it. If interested companies and business associations wish to be included in the process, their contribution must be adjudged to be valuable and that can only mean the kind of solid research, careful definition and scrupulous documentation that earns respect and convinces the other participants. That kind of meaningful contribution will not come cheaply and businessmen must be prepared to contribute sufficient resources to ensure that the debate takes place at the level of technical expertise and not at the level of vague generalities and sloganeering. Without that kind of serious commitment, the overwhelming resources of the government will prevail and the ultimate solution reached may reflect bureaucratic and political priorities rather than the imperatives of economic reality.

It is also clear that any treaty or agreement entered into between the two countries cannot hope to treat of and settle all of the problems which will inevitably arise in a trade which is so extensive, complex and fast changing as information exchange. Whatever treaty is negotiated will have to be flexible, open-ended, and susceptible to subsequent monitoring and modification.

Indeed, the two countries may consider some kind of bilateral standing group to track the implementation of the agreement and defuse complaints before they fester into major political confrontations. It may be worth remembering that every regulation offers a fixed target to the innovator who would devise some way around it. With the quickly changing technology of today, any fixed agreement would soon be overtaken by developments that rendered it obsolete. If the two countries want to negotiate a meaningful agreement on the information trade between them, they would do well to consider the advantages of an organic system such as the British constitutional tradition which enshrines basic principles and then relies on precedents and interpretations that change with the times when deciding how to apply those principles. Something like this approach may be necessary in the highly volatile environment of transborder data flows.

RETAIL BANKING

JAMES C. GRANT *
Vice-President
Strategic Planning, Retail Banking
The Royal Bank of Canada

I would like to join my fellow panelists and conference speakers in welcoming the Government of Ontario's initiative in bringing together representatives from Ottawa, the provinces and territories and the private sector to discuss privacy and related issues. I am pleased to note that the views of the private sector have been actively sought. On behalf of my business colleagues, and certainly on behalf of the Royal Bank, I am happy to contribute to the discussion of these issues.

Let me begin by trying to pin down what is meant by the phrase "transborder data flows". It was coined, if I am not mistaken, by today's Chairman, Russ Pipe, at the O.E.C.D.'s first conference on the issue in 1977. It is a bit of a catch-all that covers a complex of interrelated subjects -- from access to computer services and telecommunications standards to copyright law, broadcasting, cultural policy and privacy. I sometimes wonder if there are any activities that do not somehow relate to the transmission of information across national boundaries.

This morning, I would like to discuss two subjects that fall under the umbrella of transborder data flows. One, primarily economic, is the exchange of commercial information, technology, knowledge and computer services. The other, primarily a human rights concern, is privacy protection.

It has been suggested that economic efficiency depends on the "free flow" of information across national borders. In fact, I doubt that totally free information flows exist or even that they are desirable. Electronic highways need rules of the road. Just as technical rules are needed by computer and telecommunications engineers, rules on access to service and markets are needed to create a predictable environment for business planners. It is also evident that rules are needed to protect sensitive national interests, be they economic, cultural or legal.

There are few national interests more sensitive than that of privacy protection. Privacy is important for two main reasons.

First, in the "information age", privacy protection is important in its own right. People demand it, although it is not entirely clear what exactly they want. Abuses are possible and protection must be "built in" to information processing systems.

Second, given the volume and economic importance of transborder information flows, uniformity in the fundamental ground rules of privacy protection is important. Privacy laws, regulations and corporate codes need not always be identical. But they do need to be consistent enough to offer individuals the

---

* Mr. Grant is a professional engineer and before joining the Royal Bank of Canada in 1968, worked on the engineering side of air traffic control with the Federal Government, and in the systems area for a major oil company. He is presently Vice-President, Strategic Planning, Retail Banking for the Royal Bank. He is involved in a number of outside organizations including being the Canadian delegate to the Paris-based International Chamber of Commerce Commission on Computing Communication and Information Policy. He is a member of International Advisory panel of Transnational Data Report (Amsterdam) and a member of the Canadian Bankers' Association Payments Strategy Committee.

same basic protection of personal information, no matter where it is stored or processed.

Governments are not alone in appreciating the importance of privacy protection. Banks, for example, depend as much on public confidence as governments do on voter confidence. Our customers also happen to be governments' employers. Whether they wear consumers' or voters' hats, they are concerned with what happens to the personal information stored in the automated data bases of both business and government.

As we heard in earlier conference sessions, North American privacy legislation applies mainly to the public sector and is, in any case, still in its formative stages. This gives Canadian business what I think is a "window of opportunity" to take the initiative in developing privacy standards. These standards should be rigorous enough to provide full public confidence without introducing economic inefficiencies -- a flexible approach, in other words.

But flexibility does not mean creating loopholes and fiddling the rules. It means adapting fundamental standards of privacy protection to specific industries and organizations. For example, many bank customers expect banks to retain credit files even after a loan is retired. Part of their reason for dealing with us is to build a widely accepted credit rating which they want disclosed in appropriate circumstances and with prudent safeguards. Flexible standards are not just more economically efficient, they can also be more effective in protecting privacy.

Business realizes that if it fails to regulate itself to the public's satisfaction, it is leaving the door open to detailed government regulation. And I, for one, would be very pleased to relieve civil servants of that burden. Within my industry, the Canadian Bankers' Association and its member banks, including the Royal, are currently studying the issue of privacy protection with considerable care.

In working with government and the public to build a consensus on privacy, business will have several prime concerns in mind.

One is that the "Rules of the Road" be clear and predictable. This is essential if modern business is to make optimum use of computer technology to promote efficiency and competitiveness, particularly in international markets. Sudden changes in government policy can jeopardize large investments in equipment, research and development and systems engineering.

Another concern is that the rules be uniform within Canada. One would think that, as a matter of public policy, Canadians should have the same basic privacy rights from coast to coast. There is also a pressing economic reason for uniformity in a federal state with a small domestic market. Disruptions in inter-provincial information flows could deprive Canada of its common market in computer services. Identifying uniform privacy rights should be straightforward. More difficult, but nevertheless vital, is the uniformity of regulatory mechanisms. This will require the precise meshing of federal, provincial and private sector codes.

A third concern of business is that Canada's privacy protection rules be in harmony with those of our main trading partners, in particular the United States. Otherwise, Canadian firms could face increased risk and cost in a highly competitive environment.

The search for widely accepted principles of privacy protection should begin with the O.E.C.D. Guidelines on privacy and transborder flows of personal information. They provide valuable reference points for both international and federal/provincial harmonization. The Guidelines are gaining acceptance. They are both comprehensive and flexible enough to reflect the core of privacy rights common to codes, bills and laws in a number of countries, including Canada. The Royal Bank, among others, has urged the federal government to endorse them formally. The U.S. government and many corporations outside Canada have already done so.

I would like to spend the next few minutes on the rationale for my three prime concerns -- the need for clear privacy rules, the need for uniformity within Canada and the need for harmonization internationally. Managing these issues effectively will greatly strengthen Canada's international competitiveness. To grasp why, it is necessary to understand the growing economic importance of computerized information services.

Ready access to these services, internationally and inter-provincially, is essential to efficiency, wealth creation and output growth in all sectors of the Canadian economy. More and more industries are becoming major users of "high tech" as computer applications proliferate and the cost of data processing falls.

In the service sector, for example, which accounts for 2/3 of Canada's GNP and an ever increasing portion of world trade, computerized information systems are boosting productivity and transforming product lines and delivery systems. In manufacturing, computers are used for everything from production to market research, distribution, inventory control, product design and financial planning.

In agriculture, let me give you an example from the Royal Bank itself. Our agrologists now use portable computers to help farmers forecast cash flow using estimated crop yields, input costs and world market prices. Projections that used to take hours are done in seconds, using up-to-date computerized data on commodity prices, weather patterns and so on.

Technological advance may be creating many new cost-efficient information services and data bases. But their utility rests on ensured, uninterrupted access for users. Consider the case of Dresser Industries. You may recall that after martial law was imposed in Poland, the U.S. government prohibited that firm's French subsidiary from supplying equipment or technology for the Trans-Siberian gas pipeline. What, might we guess, happened to the economic value and reputation of Dresser France the instant it was denied access to expertise and information?

In the absence of international agreements ensuring uninterrupted access to information services, business faces an uncertain environment. There is a danger that countries will act unilaterally to restrict the kind of information that can be sent, processed or stored abroad. The result could be an array of restrictive rules and regulations, ranging from tariff and non-tariff barriers to government attempts to register, tax and monitor all data banks. The threat of information protectionism is greater for Canada, with its relatively small domestic market, than it is for larger nations and trading blocs.

For all these reasons, the Royal Bank has proposed and actively promoted the idea of a sectoral agreement between Canada and the U.S. covering what we call "traded computer services", a bilateral agreement that could set the pattern for subsequent multilateral liberalization. Our proposal is double-barrelled.

One barrel is aimed at establishing mutually acceptable trading rules governing access to markets for Canadian and American suppliers, and access to computer services for Canadian and American users. The other barrel is aimed at the harmonization of privacy protection in the two countries. I have just discussed the economic and trade issues. Let me now turn to privacy.

An international patchwork of privacy protection regimes could have much the same economic effect as overt restrictions on information trade and exchanges. Business would be confronted with the costs and inefficiencies of multiple regulatory compliance from country to country. Even worse, there is the risk that governments will insist that all personal information be processed in domestic data banks on the grounds that other countries do not offer equivalent privacy protection. Except in Europe, international ground rules on privacy are hazy. Information flows can be disrupted in arbitrary, unpredictable ways.

Another source of uncertainty has been the perceived risk that some European countries could use privacy protection

as a smokescreen for trade protectionism. Government regulators must keep privacy rights separate from trade issues. Privacy protection is complex and demanding enough that it would be unwise to mix economic problems in as well.

The notion of privacy has become quite sweeping. From a banker's perspective, the evolution is interesting. Traditionally, bankers have had to meet high public expectations concerning two aspects of privacy:

The first is "security": bank vaults are now being supplemented by the computerized "gate-keepers" protecting data bases from unauthorized access.

The second aspect is "confidentiality": bankers, like doctors and lawyers, are custodians of their clients' information. They have a contractual duty to disclose it to third parties only in very narrowly defined circumstances, principally with customer consent and under legal compulsion.

But "privacy" now goes beyond "security" and "confidentiality". It is viewed as a comprehensive set of rights that give individuals a degree of control over personal information -- not only over how it is disclosed, but also how it is collected, processed, used, verified and corrected in the event of error.

Banks are "information intensive" businesses, which need access to private personal information to do business and which need to maintain public confidence to stay in business. We are fully aware that our policies and information practices must reflect the modern concept of "privacy". Our experience with "security" and "confidentiality" is a solid foundation to build on.

It is essential not only that privacy be protected and public trust maintained, but, for the economic reasons I have discussed, that various nations' privacy requirements be reasonably uniform.

Clearly, the numerous privacy laws passed in Europe and North American are not perfectly uniform. The key differences concern enforcement methods and the scope of regulation -- whether it applies, for example, to the public sector alone or to the private sector as well, to automated information systems or also to manual files.

More important than these differences, however, is the fact that the legislation to date reflects the same basic policy concern -- to give the individual a reasonable degree of control over personal information and impose corresponding rules on governments and corporations.

Outside of Canada, it may not be realistic to implement a scheme for making all privacy laws perfectly uniform. But it is quite realistic to identify what they have in common. Herein, as I suggested earlier, lies the value of the O.E.C.D. Guidelines. They set out core principles of privacy protection that should be seen as the common measure of many countries' privacy codes, whether they are imposed by legislation, regulatory policy or voluntary compliance.

In these circumstances, the practical questions to ask are: Can countries "harmonize" their privacy policies without having identical regulatory frameworks? Can individuals be assured that their personal information will enjoy the same basic protection abroad that it enjoys in the home country? My answer to both is a qualified "yes".

One qualification is the attitude of governments. As I have suggested, they must maintain a disciplined separation of privacy from trade issues. This is an essential condition for harmonization.

Another qualification is the attitude of the private sector. Business must understand that rigorous and uniform codes for protecting privacy can go a long way towards reducing the need for government regulation. It will also reassure citizens that multinational data flows are not threatening.

Of course, no government will abandon its concern and leave the private sector to decide how and under what conditions

personal information will flow across borders. But political pressure for "me first" privacy laws will be relieved... if corporations act to put meat on the skeleton of the O.E.C.D. Guidelines... if multinationals begin to adopt uniform industry-wide or inter-corporate codes... if companies show the public that they are taking specific measures to reduce the risk that personal data will be mishandled in foreign data bases and processing centres. Such private sector actions are the raw material for more formalized harmonization of laws by governments as time goes on.

The multinational private sector should not underestimate its influence. It has long experience in operating in different political, legal and regulatory environments. It also has the knowledge of information technology which governments need to formulate sound policy.

Government action to harmonize privacy protection is most practical when it is taken by neighbouring countries, with similar legal systems. We are already seeing this in Europe. It seems to me that Canada and the U.S. could follow suit and negotiate a North American "model agreement" covering such matters as information retrieval rights, equivalent protection, mutual enforcement of court orders and agreed procedures for determining court jurisdictions when citizens of the two countries are involved.

But Canada cannot negotiate international agreements unless the federal government and provinces adopt a uniform approach to privacy protection. We simply cannot arrive at the negotiating table with our governments pulling in anywhere from two to eleven different directions on such a fundamental human rights issue.

There is also, as I mentioned before, a purely domestic imperative for uniformity. Canada should preserve its common market in the field of information flows and services. Governments should consider the business cost implications of differing regulatory regimes. Even today, minor differences in such areas as interest rate calculations and financial reporting requirements can force corporations to develop entirely different computer programs and software applications for different jurisdictions. The same problem could arise if privacy protection requirements diverge from one government to the next.

As a businessman, I do not have strong feelings about the precise definition of federal/provincial jurisdictional boundaries in the field of privacy. What is terribly important is that all Canada's governments start by "agreeing to agree" on a uniform, nationwide set of privacy rights for all Canadians. My experience is that Canadians expect to have identical privacy rights, no matter where they live or where in future they might move within Canada. If my perception is right, governments would have to be politically motivated to take a shared approach.

If agreement on privacy rights can be reached, we can then turn to the question of the respective roles of Ottawa, the provinces and territories and the private sector in ensuring that privacy rights are respected.

In attempting to arrive at a uniform regulatory framework, all governments should be alive to the role which the private sector can play. Corporations, industry associations and other private sector groups can assist government in ensuring that fundamental privacy protection principles are implemented effectively and evenly throughout the country. Effective self regulation, if it becomes integral to the enforcement of privacy rights, can assist the process of federal/provincial consensus building. For self regulation to be effective, it would have to reflect a national consensus on privacy.

Privacy protection is an important issue, one which requires extensive discussion by all interested parties. Thanks to this conference, it has been discussed in spades. Thank you for this opportunity to participate.

SUMMATION OF CONFERENCE BY RAPPORTEUR

CARL F. DOMBEK *
Director, Legal Services
Ontario Ministry of Labour

In his remarks opening the Privacy Conference, the Honourable Norman W. Sterling, Q.C., Provincial Secretary for Resources Development, challenged us to respond to the issues created by rapidly changing and increasingly sophisticated technology systems and their impact on traditional values respecting privacy. He asked us to consider both the problems we face and the options available to us for their solution and also to think about developing standards which meet our needs and bring Canada into harmony with developing world-wide standards of data protection. This Conference has responded to that challenge with panels which have aired the many perspectives on these issues and their resolution.

The first Panel was entitled "Privacy: The Problems Defined". Speakers bringing the perspectives of the manufacturing, insurance and medical communities emphasized the legal and administrative problems privacy protection presents for information keepers. These include costs incurred when information contained in personal files is subpoenaed by third parties for use in civil actions; through litigation which might have been avoided if employers had access to employee records; and inefficiencies which result from prohibitions on the surveillance of employees.

In addition, the consequences of the release of business information through Government access to information legislation was mentioned. All three panelists saw Government as the major threat to the informational privacy of individuals. This was particularly seen as true in the medical record area, where Government balances public interest concerns against individual privacy rights. Panelists saw privacy protection as now practiced in the private sector as adequate, with no additional regulations or legislation required.

Another Panel was created to deal with issues in the public sector. It was called "Access to Information: How Does This Relate to Privacy?".

In addressing this question, the Panel considered the search for balance between the need for privacy protection and access to information. Accordingly, the first speaker canvassed the various mechanisms and quirks within Canadian statutory schemes, such as the resolution of these two competing claims through the exemptions, the exclusions, and the third party intervention or reverse freedom of information procedure.

He identified the enormity of the problem of our global information society which will necessitate the development of a comprehensive and international "information law" to cope with this new information era.

Among the many issues raised was an assertion that data protection and access

---

* Presently the Director of Legal Services at the Ontario Ministry of Labour, Mr. Dombek assisted the Hon. Norman W. Sterling Q.C., Provincial Secretary for Resources Development, Ontario, in the drafting of the Province's Privacy and Access to Information Act. He is a member of the Canadian Bar Association (Ontario) Committee on Privacy and Computers. He is the author of legal articles on criminal law and is a graduate of Brock University and Dalhousie Law School.

The editor gratefully acknowledges the assistance of the Conference's two Assistant Rapporteurs, Ms. Martha Fletcher and Ms. Liz Longworth, in the preparation of this Conference summary.

to information issues reflect long-standing societal conflicts over the redistribution of power between the individual and the state. Computer technology speaks a new language of power which comes from controlling the flow of information.

The call for data protection and freedom of information law reform is another example of the increasing demand by citizens for greater participation in decision-making. Using a Charter of Rights analogy, he reflected that such reform is part of a trend in Canadian legal culture towards codification of procedural entitlements. This may reflect the public's increasing distrust of large institutions and fear of the invasion of personal privacy. The resulting explicit rights to information are vital for effective participation in an information society.

In attempting to answer the question before the Panel, the next speaker gave a comparative account of data protection and privacy laws in West Germany, France, U.K., U.S.A. and Quebec. He isolated strengths and weaknesses of these schemes, emphasizing the need to make laws effective and to deal adequately with the public sector situation before turning one's attention to the private sector. For any data protection agency, he stressed, among other things, his preference for the agency to have advisory powers only and the need for the agency to concentrate on data protection rather than becoming overwhelmed by the access issue. The speaker also mentioned the necessity to avoid duplication of commissions and bureaucracy; the need for the agency to enjoy as much independence as is constitutionally possible, subject to an appropriate review mechanism; the need for effective organization of the agency, and the importance of talented and proper staffing. He continued by discussing the need to define the actual privacy interests to be protected; and he stressed the need for the agency to be empowered to receive complaints, initiate audits and inspections, and generally to be visible and seek to implement data protection laws in an effective manner.

Finally, the more technical problems involved in the integration of the two schemes (privacy and access) were addressed with some suggestions as to how one might reconcile the conflict between the two.

For the designers of legislation, there appear to be three policy problems: the first, the focus of conflict resolution, that is, which institutions (Courts, Legislature or Bureaucracy) decide the issue. Second is the substantive policy question as to what guidance can be given to the decision-maker to assist in resolving the conflict. Third are the technical problems of drafting to avoid conflicts within the statutory schemes, as is found in the Canadian Federal Access to Information and Privacy Acts.

After a comparative look at the U.S. law, it was concluded that the Canadian approach in effect leaves the resolution of this conflict within the discretion of public officials, thereby undermining access rights conferred by the Access to Information Act and depreciating the level of privacy afforded by the Privacy Act.

Despite the Canadian and U.S. approaches, the speaker believed that is is possible to articulate a number of precepts which could assist a decision-maker in resolving the access and privacy conflict. He proceeded to set out at least 10 principles, thereby illustrating that there is a practical solution to this whole question of achieving the appropriate balance in reconciling privacy protection with the freedom of information principle.

The question period concentrated on the appropriate role of the Privacy Commissioner; whether the Commissioner should or should not be a citizen's advocate; the need for more consciousness raising in data protection by the Commissioner initiating inspections of files; the need for increased publicity and education campaigns, and the importance of controversy as a solution to the lack of publicity.

A third Panel dealt with "Privacy: What the Private Sector Has Done". both morning and afternoon private sector

sessions spoke on the question of what the private sector has done to respond to privacy concerns. The insurance industry, for example, collects less information and, in particular, less subjective information than in the past.

The industry provides for easy correction of its information and maintains tighter security on what is collected. Both individual corporations and industry associations were able to report on work done to achieve self-regulation through development and implementation of codes of fair information practices. Some commentators questioned the view that privacy was a real concern of citizens, arguing that dealings in the private sector are voluntary in any case. Others pointed out that while many small invasions of privacy were tolerable in isolation, the cumulative effect -- particularly when magnified through linkage of files -- is substantial and of widespread concern. As well, for most individuals, "opting out" of the information society is not a realistic possibility. Finally, self-regulation provides no means for dealing with the irresponsible firm or with those who are not members of industry associations and have no incentive to accept their codes. Therefore, discussions of regulatory options cannot be avoided.

In dealing with "Privacy: Some Practical Solutions", the other afternoon Panel tackled the privacy issue more directly by looking to other jurisdictions for some practical solutions. In the course of looking at the American legislation, the issue of computer-matching and computer crime security were discussed. Some of the recommendations were: to use computer technology in order to implement fair information practices and computer security; to recognize the necessity for follow-up audit or evaluation of policy and safeguards in the new statutes; and to improve upon drafting, such as by eliminating the routine use disclosure provision. The panelist suggested the establishment of an entity with the resources to implement these recommendations, as well as to embark upon long-range planning. He pointed out various situations, such as medical research, where matching is legitimate so long as accompanied by safeguards. Stressing the importance of due process and verification procedures, it was concluded that is is still possible to use advanced technology, to have an efficient administration and yet still protect the privacy rights of citizens.

The issues under discussion in Saskatchewan where there is no statute were then examined, with reference to some of the options available in other jurisdictions. The desirability of finding an appropriate model which would avoid over-regulation by government, was expressed. Pointing out the need to think in terms of new forms of privacy, this speaker said that his concern was misuse of information, rather than with the fact of data collection per se. To illustrate his points, he drew on his Province's experience with the system of the Pathfinders Trail and Agritex Service. We then heard a detailed account of the Quebec access law which comes into effect this July. Quebec is the only province with data protection legislation. Five characteristics of the new law were identified.

1. The legal aspects, whereby freedom of information and data protection are guaranteed within the same Act,

2. The coverage of the Act is very extensive, affecting 3,600 agencies, as opposed to 140 in the Federal Act; it includes all Crown Corporations and covers confidential files in the federally "exempt " category,

3. Data linkage between agencies is regulated with the host agency restricted in releasing personal information to another unless under the terms of an agreement which has to be tabled in the Assembly,

4. The 3-member commission is a hybrid body with regulatory and advisory functions,

5. The distinguishing characteristic of the law will be its high degree of elaboration and resulting bureaucracy.

Another Panel was entitled "Privacy: Initiatives for the Private Sector". As the Chairman of this Panel noted, one objective of this Conference is to hear from representatives of the public -- those most affected by the changes leading to an information society. To that end representatives of labour and consumers discussed the issues of greatest importance to them, in effect challenging public and private sector data holders alike to find adequate responses to their concerns. For consumers, these include defining the balance between privacy and access to information; ensuring that transborder data flows do not rob Canadians of effective control of data-handling practices; and restricting information use to the purposes for which it was collected. In addition, it was suggested what we should encourage the development of "informed consent" which should be coupled with a right of refusal which does not exact onerous penalties for its exercise. For labour, major issues are the misuse of personnel information by employers, and the use of new technologies for surveillance of employees. For all panelists, a major issue is information use and collection by Government, and the use of the social insurance number as an all-purpose identifier. The final panelist, representing the Canadian Independent Computer Services Association, argued that the only solution for such problems is a legal one, as lack of effective sanctions merely gives economic advantage to the least scrupulous.

On May 24th, the delegates participated in a Panel entitled "Transborder Data Flow: Toward a Resolution for the Future: The Trends, the Issue".

The speakers discussed the impact of the development of significant levels of transborder data flow on the capacity of Canada's governments to achieve economic, cultural and human rights goals and on the means available to them to do so. The solution offered was for Canada to come to terms with its major trading partner, the United States.

Such discussions have begun with the current Canada/U.S. discussions of sectoral liberalization, where informatics is identified as a sector for such agreement. While the bilateral approach is seen as offering the best hope for actually achieving agreement, a number of issues need resolution. First, information is an input, not a sector, and as such, it affects all sectors. Thus, its effect in each sector must be assessed in the negotiation process. Other issues include control of carriage,acceptable forms of documentation, liability for defects, security of information, and extraterritorial effects of data protection laws. These negotiations will succeed only if the essential focus of agreement can be narrowed and there is the political will to create structures for adjustment of the agreement to meet the changing environment. Without a continental communication pact, Canada will lose its already weak position with regard to hardware technology and software. It is up to Canadian policy-makers to explore the opportunities to secure Canadian privacy, sovereignty and employment opportunities in the Information Age.

The delegates also heard from two excellent keynote speakers during the Conference. Federal Privacy Commissioner John Grace was able to report that the Federal Privacy Act is, in its first year of operation, working better than expected. Some 10,000 requests for information were received in the first six months, with 80% of applicants receiving at least some of the information requested. His Office has been used as a clearing house for questions regarding privacy practices as well.

Later, the Honourable David Waddington told the group that the United Kingdom Data Protection Bill, now before Parliament and soon to become law, was conceived in response to two important pressures: first, the growing public concern about the impact of automatic data processing on individual privacy, and secondly, the concern in the private sector that absence of a law would hamper data flows to the U.K. from European countries which adhered to the Council of Europe Convention on Data Protection. The British Bill covers only computerized data banks but includes both the public and private sectors. Data users will register their

data banks, and a Data Protection Registrar will oversee the operation and enforcement of the Act.

In conclusion, the delegates heard that Mr. Sterling would be introducing a Bill concerning Privacy and Access to Information held in Government data banks. The delegates are also aware that the Provincial Secretary is chairing an Inter-Provincial Minister's Conference, which will discuss the issues of privacy in the private sector. The delegates want to emphasize to the Ministers that it is important, in fact necessary, to continue consultation with the private sector at all stages prior to Government taking any final action on the subject.

As a final word, many delegates expressed their satisfaction that the Government was interested in this topic and they hoped that this interest would not wane. There was also a general expression of thanks to the Government for bringing the delegates together on May 23rd and 24th of this ausipicious year.